The Boeing Company

Certificate Policy

NOTE: Although this CP includes the Boeing Medium Assurance Hardware Domain requirements, a separate Boeing Medium Assurance Hardware Domain CP MUST be used and is still in effect until further notice. The Boeing Medium Assurance Hardware Domain CP can be found here: http://crl.boeing.com/crl/

Version: 1.3
Release Date: 12/5/2023
Boeing PKI Policy Authority Board Approved: 12/19/2023

CP Version Information

Method of Approval: Roll Call / E-Mail Vote	Date of Approval	Version Number	Change Request (CR) / Revision Record (RR)
E-Mail Vote	12-09-2019	1.0	TFS CR 26610 New Release
Roll Call / E-Mail Vote	1/28/2022	1.1	TFS CR 182620 RR_2022-01
Roll Call / E-Mail Vote	12/15/2022	1.2	TFS CR 269569 RR_2022-02
Roll Call / E-Mail Vote	12/19/2023	1.3	Ticket 317274 RR_2023-01

Table of Contents

1. Introductions

This certificate policy (CP) defines the requirements for Public Key Infrastructure (PKI) operated by The Boeing Company in order to:

1. Enable authentication;
2. Enable encrypted network communications;
3. Encrypt or digitally sign digital content; and
4. Establish trust and ensure interoperability with other external PKIs (e.g., CertiPath Bridge Certification Authority for interoperation among Aerospace PKIs).

This CP is consistent with the Internet Engineering Task Force (IETF) Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework as described in Request for Comments (RFC) 3647 and organizes contents into the following nine primary sections:

1. Introductions
Identifies and introduces requirements and indicates types of entities and applications.

2. Publication and Repository
Stipulates publishing responsibilities, frequency of publication and access control of published practices, certificates, and current status of certificates.

3. Identification and Authentication
Describes the procedures used to authenticate the identity and/or other attributes of an end-user certificate applicant to a Certification Authority (CA) or Registration Authority (RA). In addition, describes the procedures for authenticating the identity and criteria for accepting applicants of entities seeking to become CAs, RAs, or other entities operating and/or interoperating with the PKI. It also includes authentication procedures for renewal, re-key or revocation requests.

4. Certificate Life-Cycle (CLC) Operational Requirements
Specifies requirements for Root and Issuing CAs, RAs, subscribers, or other participants with respect to the life-cycle of a certificate.

5. Facilities, Management, and Operational Controls
Describes non-technical security controls such as physical, procedural, and personnel controls to securely perform key generation, subject authentication, certificate issuance, certificate revocation, auditing, and archiving.

6. Technical Security Controls
Describes the security measures taken by the CAs to protect its cryptographic keys and activation data (e.g., PINs, passwords, or manually-held key shares). It may also impose constraints on repositories, subscribers, and other participants to protect their private keys, activation data for their private keys and critical security parameters. In addition, it describes other technical security controls to securely perform key generation, user authentication, certificate registration, revocation, auditing, archiving, and other operational controls.

7. Certificate, CRL, and OCSP Profiles
Specifies certificate, CRL and/or OCSP formats (e.g., profiles, versions, and extension usage).

8. Compliance Audits and Other Assessments
Identifies topics covered by or methodology of the compliance audit and/or assessment. It also contains compliance audit/assessment frequency or triggers for such, compliance audit/assessment personnel stipulations, required actions for deficiencies discovered and compliance audit/assessment report privileges and communications.

9. Other Business and Legal Matters
Addresses business and legal matters consisting of general matters, various services fees, and financial responsibilities of participants for ongoing operations and for paying judgments or settlements. Other legal topics are included and MAY or MAY NOT mean the CP is considered a contract or part of a contract.

1.1 Overview

The Boeing CP is the policy under which all Certification Authorities and other supporting PKI components operated by The Boeing Company are established and operated. This CP and certificate profile documents located on the PKI Repository (see glossary for PKI Repository URL) further define the policies applicable to the use of digital certificates issued by the Certification Authorities governed by this CP. Certification Authorities under this CP support Levels of Assurance (LoAs) measured by the strength and rigor of the identity proofing process, the credential's strength, and surrounding controls of the PKI.

The word "assurance" in this CP means:

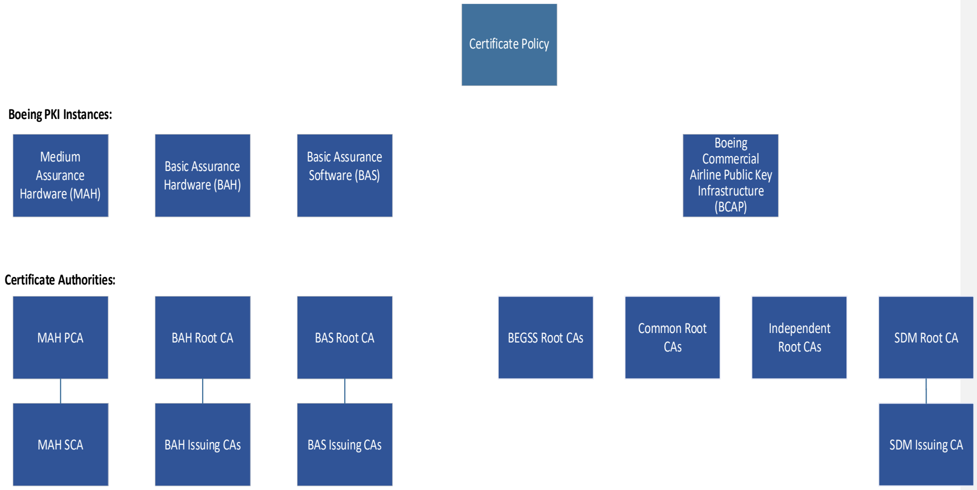
1. How well a Relying Party can be certain of the identity binding between the public key and the entity (human and non-human) whose subject name is cited in the certificate;
2. It reflects how well the Relying Party can be certain that the entity (human or non-human) cited in the certificate is controlling the use of the private key that corresponds to the public key in the certificate; and
3. How securely the system which was used to produce the certificate or Certificate Signing Request (CSR) performs its task and (if appropriate) delivers the private key to the end entity or end entity Sponsor.

Assurance levels of The Boeing Company Certification Authorities are categorized as:

4. Basic assurance (hardware and software [software includes Boeing Commercial Airline PKI]); and
5. Medium assurance (hardware and software).

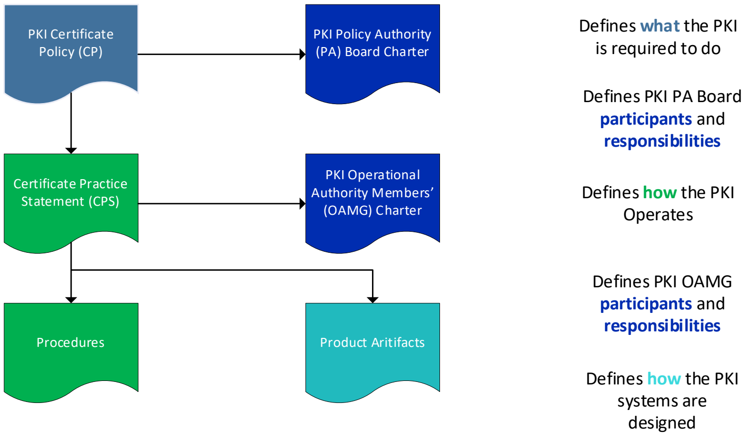
A certificate practice statement (CPS) MAY further define LoAs leveraging NIST SP 800-63.

1.1.1 Certificate Policy Relationship to Certification Authorities



1.1.2 Relationship between this CP and Other Artifacts

The diagram below depicts the relationship between this CP, Boeing PKI governing entities, and other artifacts such as Boeing policy, practice statements (certification practice statements [CPSs] and key recovery practice statements [KRPSs]), procedures, and product documentation.


PKI Certificate Policy (CP)
PKI Policy Authority (PA) Board Charter
Certificate Practice Statement (CPS)
PKI Operational Authority Members' (OAMG) Charter
Procedures
Product Aritifacts
Defines what the PKI is required to do
Defines PKI PA Board participants and responsibilities
Defines how the PKI Operates
Defines PKI OAMG participants and responsibilities
Defines how the PKI systems are designed

1.1.3 Scope

The scope of this CP:

1. SHALL include all Boeing PKIs and their supporting PKI components operated by The Boeing Company. See section 1.6, Definitions and Acronyms for definition supporting PKI components.

1.2 Document Name and Identification

This document is called The Boeing Company Certificate Policy. The Boeing Company is assigned a private enterprise object identifier (OID) of 1.3.6.1.4.1.73 by the Internet Assigned Numbers Authority (IANA), which Boeing has further refined into sub-arcs:

Reference	Object Identifier (OID)	Source
The Boeing Company	1.3.6.1.4.1.73	IANA
Boeing Information Security	1.3.6.1.4.1.73.15	Boeing
Boeing Public Key Infrastructure	1.3.6.1.4.1.73.15.3	Boeing
Boeing Certificate Policies	1.3.6.1.4.1.73.15.3.1	Boeing
The Boeing Company Certificate Policy	1.3.6.1.4.1.73.15.3.1.18	Boeing

The following OIDS are Certificate Policy (CP) document mapped as indicated below:

Reference (Certificate Policy documents)	OID	Certificate Policy Document Mapping
Basic Assurance Hardware CP	1.3.6.1.4.1.73.15.3.1.7*	1.3.6.1.4.1.73.15.3.1.18
Boeing Class 2 CP (BAS)	1.3.6.1.4.1.73.15.3.1.2*	1.3.6.1.4.1.73.15.3.1.18
Boeing Commercial Airline PKI CP	1.3.6.1.4.1.73.15.3.6* (SDM) 1.3.6.1.4.1.73.15.3.6.3* (BEGSS)	1.3.6.1.4.1.73.15.3.1.18

*These OIDs referenced are for retired Certificate Policy documents and will remain in the existing CA certificates but new CA certificates issued after 1-10-2022 SHALL use the Boeing Certificate Policy OID 1.3.6.1.4.1.73.15.3.1.18. End entity certificates issued after 1/10/2022, if using a Policy OID, SHALL use the Boeing Certificate Policy document OID 1.3.6.1.4.1.73.15.3.1.18 in the Certificate Policies extension.

Additional OIDs and their particular purpose(s) can be found in certificate profile documents located on the publicly-facing PKI Repository (see section 1.6 of this CP for the PKI Repository URL).

1.3 PKI Participants

1.3.1 Certification Authorities

A Certification Authority (CA) issues certificates to subjects. A CA is a required component in a Boeing PKI environment. Boeing PKI SHALL utilize one or more of these four types of CAs:

1. A Principal CA (PCA) is a Root CA operated that is designated to cross-certify directly with the third-party bridge CA through the exchange of cross-certificates. A Boeing PCA is authorized by the Boeing PKI Policy Authority Board to create, sign and issue public key certificates to Boeing Subordinate CAs to issue subscriber certificates;
2. A Root CA is a self-signed CA that serves as a trust anchor for a Boeing-operated PKI. A Root CA manages and publishes certificate for Issuing CAs;
3. A Subordinate CA (SCA) which is signed by a PCA. An SCA manages and publishes certificates for human and non-human subjects; or
4. An Issuing CA which is signed by a Root CA. An Issuing CA manages and publishes certificates for human and non-human subjects.

1.3.2 Certificate Status Authorities

A Certificate Status Authority (CSA) MAY be implemented to provide status of certificates or certification paths. A CSA:

1. SHALL use Online Certificate Status Protocol (OCSP) or MAY use a Simple Certificate Validation Protocol (SCVP) Server;
2. SHALL require OCSP Responders to be issued CA-delegated certificates(s) as specified in section 2.6 of RFC 6960 in order to ensure interoperability with cross-certified partners;
3. SHALL adhere to the same security requirements as repositories if the OCSP Responders are keyless and simply repeat responses signed by other Responders; and
4. MAY be operated in conjunction with an entity's CAs or independent of the CAs.

1.3.3 Identity Authorities

Identities MAY be validated using Identity Authorities that are the authoritative sources for the identifier and related identity attributes for a subscriber.

1.3.4 Registration Authorities

A registration authority (RA) SHOULD be used in a Boeing PKI environment. An RA:

1. SHALL establish enrollment processes for certificate subscribers;
2. SHALL perform identification and authentication of certificate subscribers using authoritative sources;
3. SHALL process certificate requests using approved secure protocols on behalf of the subscriber;
4. SHOULD approve applications or renewal or re-keying certificates either for or on behalf of human and non-human subjects; and
5. SHOULD Initiate or pass along revocation requests for certificates.

1.3.5 Trusted and Administration Workstations

Trusted and Administration Workstations (see glossary) are restricted workstations. They:

1. SHALL be used to administrator PKI components or supporting PKI components from a specific secure location inside or outside the security perimeter as described in an applicable CPS.

1.3.6 Sponsor

A Sponsor fills the role of a subscriber for non-human end entities that are named as public key certificate subjects. The PKI Sponsor:

1. SHALL meet the obligations of Subscribers as defined throughout this document;
2. SHALL verify the subscribers have an approved business relationship with The Boeing Company;
3. SHALL work with the RAs to identify the authoritative source of the subscriber;
4. SHOULD use a credential that is commensurate with the level of the certificate they are sponsoring; and
5. SHOULD submit certificate requests, revocation requests, or renewal requests on behalf of non-human subscribers.

1.3.7 Subscribers

A subscriber is a human or non-human entity requiring a certificate that maintains a business relationship with Boeing. Subscribers:

1. SHALL be issued certificates from a Boeing-operated CA; and
2. SHALL use a certificate to assert a claimed identity to relying parties.

1.3.8 Relying Parties

A Relying Party is the entity (e.g., person, organization, system) that trusts a Boeing-operated PKI to authenticate and bind to a subscriber. Relying parties MAY use this binding for cryptographic operations such as:

1. Authenticating a subscriber;
2. Verifying the integrity of a message digitally signed by the subscriber;
3. Confirming a message originated from the subscriber; or
4. Establishing confidential communications with the subscriber.

1.3.9 Other Participants

1.1.1.1 Boeing PKI Policy Authority Board

The Boeing PKI Policy Authority (PA) Board comprises executive stakeholders representing the interests of PKI for Boeing and provides oversight of the Boeing PKI Operational Authority. The voting members approve the strategic direction for PKIs, changes to the CP as well as changes to the PKI trust relationships between Boeing and other external PKIs. The Boeing PKI PA Charter further defines the Boeing PKI PA Board's:

1. Objectives;
2. Membership; and
3. Responsibilities.

1.3.9.5 Boeing PKI Policy Authority (PA) Chair

The Boeing PKI Policy Authority Chair is the manager responsible for the governance and oversight of PKI operations at Boeing. This individual facilitates the Boeing PKI PA Board and Operational Authority Members' Group (OAMG) meetings and other activities.

1.3.9.6 Boeing PKI Operational Authority Members' Group

The Boeing PKI Operational Authority Members' Group (OAMG) comprises managers representing the operational authority of the Boeing PKI. The voting members provide management oversight of day-to-day Boeing PKI operations. The Boeing OAMG approves changes to CPSs and KRPSs and ensures alignment of PKI practices and operations satisfy the requirements defined in this CP. The Boeing PKI OAMG Charter further defines the Boeing PKI OAMG's:

1. Objectives;
2. Membership; and
3. Responsibilities.

1.3.9.7 Boeing PKI Operational Authority Administrator

The Boeing PKI Operational Authority Administrator (OAA) is the individual appointed by the Boeing PKI Policy Authority Chair who has principal responsibility for overseeing the proper operation of the PKI environment within the Boeing PKI Operational Authorities' area of responsibility.

1.3.9.8 Boeing PKI Operational Authority

The Boeing PKI Operational Authority (OA) consists of organizations that operate the Boeing PKI and supporting PKI components. The Boeing PKI OA is responsible for all operations required for the Boeing PKIs.

1.3.9.9 Change Board

A Change Board is responsible for tracking requests to create or enhance the PKI products or services within the OA's area of responsibility.

1.3.9.10 Related Authorities

The CAs operating under this CP MAY require the services of other security, community, and application authorities.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

Certificate usage SHALL align with the intended usage specified in the applicable certificate profile located at the PKI Repository (see section 1.6 of this CP for the PKI Repository URL).

1.4.2 Prohibited Certificate Uses

A certificate SHALL be prohibited from being used after it has been suspended, revoked, or used in any way inconsistent with the key usage, extended key usage, or basic constraints specified in an applicable certificate profile.

1.5 Policy Administration

1.5.1 Organization Administering this CP

The Boeing PKI Policy Authority Board is responsible for all aspects of this CP.

1.5.2 Contact Person

Any questions or inquiries can be directed to:

Attn: Boeing PKI Policy Authority Chair
Mail Code 8J-206
PO Box 3707
Seattle, WA 98124-2207

1.5.3 Person Determining Certification Practice Statement Suitability for the Policy

The determination of suitability of a CPS to this CP SHALL be based on:

1. Review, approval, and recommendations by the Boeing PKI OAA; and/or
2. An independent Compliance Auditor's results and recommendations.

1.5.4 Approval Procedures

Approval procedures for the instantiation of this CP were submitted to the Boeing PKI PA Board by the Boeing PKI OAA and adhered to the Boeing PKI PA Board's voting process stipulated in the Boeing PKI PA Board Charter.

Subsequent CP approvals (i.e., amendments) procedures are described elsewhere in this CP.

1.5.5 Waivers

Waivers to this CP are not permitted.

1.6 Definitions and Acronyms

Activation Data - Data (other than the keys themselves) that is used and needed to activate a private key. Examples include a Personal Identification Number (PIN), password, or portion of a key or other data used to enforce multi-person control over a private key.

Administration Workstation - Restricted workstations (i.e., MAH cross-site SLS laptops, Zero Clients) used to access other PKI components.

AES - Advanced Encryption Standard.

AIA - Authority Information Access.

Audit Data - Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NIST Computer Security Resource Center, Glossary, "audit trail"]

Audit Logs - The log of activity that is being performed by a user, system, or supporting procedural process based on assertions in this CP.

Audit Logs of Record - Processed audit logs required to be archived to an archive location and maintained by Audit Administrators until archived.

Authentication - The act of verifying and validating identities.

Authorization - The granting of permissions of use.

Binding - The process of associating two related elements of information. [NIST Computer Security Resource Center, Glossary, “binding”]

CA - A Certification Authority is a trusted entity that issues and manages digital certificates (x.509) and Certificate Revocation Lists (CRLs).

Certificate - The public key of a user, together with related information, digitally signed with the private key of the CA that issued the certificate. The certificate format is in accordance with International Telecommunication Union (ITU)-T Recommendation X.509. Typically, certificates are used to verify the identity of an individual, organization, or device. They are also used to ensure message integrity through private key signature and enable confidentiality of data through public key encryption.

Certificate Chain - An ordered sequence of certificates that, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.

Certificate Life-Cycle - The finite lifespan from certificate issuance to revocation or expiration.

CMS - A Credential Management System (CMS) (otherwise known as a Card Management System) is used to encode, track, maintain, and revoke credentials as an application of a Registration Authority (RA).

Commercial Agreement(s) - Are commercial agreements between Boeing and other parties such as Master Services Agreement(s); Memorandums of Agreement(s); or Trust Agreement(s).

CP - A Certificate Policy (CP) sets forth the requirements and standards imposed on the PKI and key participants.

CPS - A Certification Practice Statement (CPS) identifies the controls and practices necessary to meet the requirements stated in the CP for each CA.

Critical Certificates - Certificates issued to Root CAs and Issuing CAs, Enrollment Agent Certificates, Qualified Subordination Signing Certificate (QSS), Content Signer Certificates, and Key Recovery Agent Certificates.

Critical Keys - HSM keys, CMS Keys, Master Keys, Root keys and Issuing Keys.

CRL - Certificate Revocation List.

Cross-Certificate - A Certification Authority (CA) certificate where the issuer and the subject are different CAs. CAs issue cross-certificates to other CAs as a mechanism to authorize the subject CA's existence.

CRL - Certificate Revocation List

Cryptographic Keys - A key is a piece of variable data that is fed as input into a cryptographic algorithm to perform one such operation. In a well-designed cryptographic scheme, the security of the scheme depends only on the security of the keys used. Includes HSM keys, CMS keys, and Master Keys.

Cryptographic Module - The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS 140-2]

CSA - A Certificate Status Authority (CSA) provides status of certificates or certification paths.

CSR - Certificate Signing Request.

ECDH - Elliptic Curve Diffie-Hellman.

ECDSA - Elliptic Curve Digital Signature Algorithm.

End Entity - The holder of a non-CA private key and corresponding certificate, whose identity is defined as the Subject of the certificate.

Entity - People and Organizations.

FIPS - Federal Information Processing Standard.

HSM - Hardware Security Module.

Issuing CA - In the context of a particular certificate, the issuing CA is the CA that issued the certificate (see also Subject CA).

KRPS - A Key Recovery Practice Statement (KRPS) identifies the controls and practices to meet requirements in the CP (in lieu of a Key Recovery Policy document) for a Key Recovery System.

LoAs - Levels of Assurance.

MAH - Medium Assurance Hardware.

Monitoring Components - Monitoring hardware, software and data on all systems used to directly support the PKI environment.

Network Components - Routers, firewalls, and switches used to directly support the PKI environment.

NIST – National Institute of Standards and Technology.

Non-Boeing Personnel - Any person or legal entity that is not a Boeing employee but has a relationship with Boeing (e.g., suppliers, Boeing purchased services, contract labor personnel, customers, and consultants).

OA - Operational Authority (Boeing PKI Operational Authority).

OAA - Operational Authority Administrator (Boeing PKI OAA).

OAMG - Operational Authority Members' Group (Boeing PKI OAMG).

Object Identifier - The unique alphanumeric identifier registered under the International Organization for Standardization (ISO) registration standard to reference a standard object or class. Object identifiers are also registered internally by Boeing.

OCSP - Online Certificate Status Protocol.

PA - Policy Authority (Boeing PKI PA Board).

PKI - Public Key Infrastructure.

PKI Component - Certification Authorities (CAs), Registration Authorities (RAs), and in some references in this CP, it may include monitoring components and network components.

PKI Repository - http://crl.boeing.com/crl/ contains information and data maintained by the PKI Operational Authority relating to systems and certificates as specified in this CP. Some may also refer to as a directory; in this CP, "Repository" refers to "PKI Repository." The PKI Repository hosts the Boeing Medium Assurance Domain Certificate Profiles document; all other Boeing PKI Certificate Profile documents (i.e., for Boeing Basic Assurance Hardware and Boeing Basic Assurance Software [including Boeing Commercial Airline PKI]) can be obtained by contacting the Boeing PKI PA Chair (see section 1.5.2 of this CP).

RA - Registration Authority (RA) is responsible for identification and authentication of certificate subjects, but does not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of an authorized CA).

Representative - In the context of this CP, a representative is an authorized entity designated to represent the organization throughout the certificate life-cycle.

Requestor - In the context of this CP, a requestor references an entity making the request to the CA/RA as a Sponsor or subscriber.

Representative - In the context of this CP, a representative is an authorized entity designated to represent the organization throughout the certificate life-cycle.

RSA - Rivest–Shamir–Adleman.

RFC - Request for Comments (document).

SCVP - Simple Certificate Validation Protocol used to validate certifications paths or provide revocation status checking services.

Security Assessments - Penetration testing, host assessments, network assessments, vulnerability assessments.

Security Containers - Physical secured storage (e.g., safes, lockable equipment racks, physical key management systems).

Sensitive Data - The subset of Boeing Information that requires specific access authorization to protect its confidentiality and also have a requirement for knowledge of, access to, or possession of the information.

SHA - Secure Hash Algorithm.

SSL - Secure Socket Layer.

Subscriber - A human or non-human entity requiring a certificate that maintains a business relationship with Boeing.

Subscriber Agreement - Signed by a subscriber or sponsor that they represent and warrant terms and conditions of being issued and using Boeing-issued digital certificates.

Subject CA - Is the CA whose public key is certified in the certificate.

Supporting PKI Components - Servers, Certification Authorities, Registration Authorities, Certificate Status Authorities, Credential Management Systems, Administration Workstations, Trusted Workstations, PKI Repositories, Cryptographic Modules.

TDES - Triple Data Encryption Standard.

TLS - Transport Layer Security.

Tokens - Hardware devices (SecureBadge, Identity Smartcards, HSM cards) that store digital certificates and private keys securely.

Trusted Workstation - Restricted workstations (i.e., CMS workstations [such as MAH Trusted Agent and Key Recovery, Badge Operator, Enterprise Help Desk and Executive End User Support workstations] and SLS laptops [non-Zero Clients]) used to access PKI components.

2. Publication and Repository Responsibilities

2.1 Identification of PKI Repository Operators

PKI Repositories SHALL be operated by those with approved authority to administer the repository host.

2.2 PKI Publishing Responsibilities

The following SHALL be published for Relying Parties and subscribers via an HTTP URL:

1. This Certificate Policy (CP) published to an HTTP URL;
2. CA certificates and certificate profiles asserting this CP published to an HTTP URL or as indicated in section 1.6 of this CP, PKI Repository;
3. Public key information when needed for authentication or encryption published to an HTTP URL or an appropriate electronic Boeing directory; and
4. Certificate Revocation Lists (CRL) published to an HTTP URL.

The following SHALL NOT be publicly published due to the sensitive nature of the information, but can be made available on a need-to-know basis:

5. Certification Practice Statements (CPSs);
6. Charters;
7. Memorandum of Agreements (MOAs);
8. Key Recovery Practice Statements (KRPSs);
9. Operating processes or procedures; or
10. Trust Agreements.

2.3 Time or Frequency of PKI Publications

The PKI Repository:

1. SHALL publish this CP when created, changed, and approved upon approval;
2. SHALL publish certificate profiles when created, changed, and approved;
3. SHALL publish CA certificates when created, changed, requested, and approved;
4. SHALL publish public key information when needed for authentication or encryption upon certificate issuance;
5. SHALL publish Certificate Revocation Lists (CRL) until all issued certificates have expired, and as based on CA assurance level, as specified elsewhere in this CP; and
6. SHOULD be available 24 hours per day, 365 days per year.

2.4 Access Controls on PKI Published Information

The PKI Repository:

1. SHALL allow write access to only authorized individuals; and
2. SHALL allow read access to others.

3. Identification and Authentication

3.1 Naming

3.1.1 Types of Names

Names used to identify the subscriber:

1. SHALL be recorded in the subject; or
2. SHOULD be recorded in the subject alternate name.

3.1.2 Need for Names to Be Meaningful

The subject name:

1. SHALL uniquely identify the subscriber (human or non-human) that is associated with the certificate; and
2. SHOULD represent the subscriber in a way that is easily understandable by humans.

3.1.3 Anonymity or Pseudonymity of Subscribers

Names for subscribers:

1. SHALL NOT allow anonymous identities;
2. SHALL NOT allow pseudonymous identities for CAs; and
3. MAY allow pseudonymous identities for human and non-human end entities to meet local privacy regulations as long as such name is unique and traceable to a corresponding unobscured name.

3.1.4 Rules for Interpreting Various Names Forms

Rules for interpreting name forms:

1. SHALL use the appropriate industry accepted standards as defined elsewhere in this CP; and
2. SHALL be clarified in a certificate profile.

3.1.5 Uniqueness of Names

Name uniqueness:

1. SHALL be enforced across the name space; and
2. SHALL be enforced across cross-certified domains.

3.1.6 Recognition, Authentication, & Role of Trademarks

Certificates issued under this CP SHALL NOT use names in their certificate requests that infringe upon the Intellectual Property Rights of others.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

Method to prove possession of private keys:

1. SHALL implement a cryptographically secure mechanism;
2. SHALL ensure the private key is bound to the identity being asserted by the subscriber; and

3. SHOULD use processes where subscribers generate their own key pairs.

CAs that issue medium assurance credentials have the following additional requirement:

4. SHALL prove possession of the private key, which corresponds to the public key in the certificate request.

3.2.2 Identification and Authentication for Organizational Identity

Identification requests:

1. SHALL include the organization name;
2. SHALL provide documentation of existence of the organization (e.g., articles of incorporation or corporation number); and
3. SHALL validate the existence of the organization (e.g., Dun and Bradstreet [DUNS] identifier; Tax authority; country, state or province corporate registry).

Authentication performed:

4. SHALL verify the information provided above;
5. SHALL verify the authenticity of the requesting representative;
6. SHALL ensure the requesting representative has the authority to act in the name of the organization; and
7. SHALL approve issuance of a certificate to the organization.

3.2.3 Identification and Authentication Requirements for Individual Identity

Identification:

1. SHALL use one or more types of identification documents for human subscribers from authoritative source(s) of identity depending on the level of assurance of the CA;
2. SHALL use one or more types of identification/registration repositories for non-human subscribers from authoritative source(s) of identity depending on the level of assurance of the CA; and
3. MAY be a previous issued credential (antecedent).

CAs that issue medium assurance credentials have the following additional requirements:

4. SHALL require subscribers present one valid and National Government-issued photo ID or two valid non-National Government IDs plus a recent photo ID and personally present identification documents to a Trusted Agent; or
5. MAY require subscribers present the above via an approved supervised remote identity proofing as approved by NIST SP 800-63A, Identity Resolution, Validation, and Verification with a Trusted Agent.

Authentication performed by RAs and to the extent possible CAs:

6. SHALL ensure all applicants' identity information is validated and from an approved source;
7. SHALL verify the authenticity and authority of the requestor;
8. SHALL ensure the applicant's identity information and public key are bound properly; and
9. SHALL record the process that was followed for issuance of each certificate.

Human subscribers:

10. SHOULD use Boeing-approved multi-factor authentication.

3.2.4 Non-Verified Subscriber Information

Information that is not verified SHALL NOT be included in certificates.

3.2.5 Validation of Authority

Before issuing certificates, validation of authority is performed as described below.

CAs that issue medium assurance and basic assurance hardware credentials:

1. SHALL have an RA validate the individual's authority to act in the name of the organization for certificates or signature certificates that assert organizational authority; and
2. SHALL have the Boeing PKI OAA validate the subject CA certificate requestor's authorization for cross-certificates to third-party bridges.

CAs that issue basic assurance credentials:

3. SHALL have an RA validate, derived validation is permissible for subscribers (end entities), the individual's authority to act in the name of the organization for certificates or signature certificates that assert organizational authority.

3.2.6 Criteria for Interoperation

Boeing CAs operating under this CP SHALL certify other CAs (including cross-certification) only as authorized by the Boeing PKI Policy Authority Board.

The following requirements MUST be completed by CAs requesting cross-certification approved by the Boeing PKI Policy Authority Board:

1. SHALL have a successful mapping of this CP with the cross-certified subject CP;
2. SHALL have a CP mapped to, and determined by the Boeing PKI Policy Authority Board to be in conformance with this CP; or in the case of subordinate CAs, the CA SHALL adopt this CP and implement a CPS;
3. SHALL operate a PKI that has undergone a successful compliance audit as asserted elsewhere in this CP;
4. SHALL issue certificates compliant with the profiles described in certificate profile documents; and
5. SHALL make certificates and certificate status information available to relying parties through a public repository in compliance with this CP.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

Identification and Authentication for routine re-key will be the same as defined elsewhere in this CP.

3.3.2 Identification and Authentication for Re-key After Revocation

Identification and Authentication for routine re-key will be the same as defined elsewhere in this CP.

3.4 Identification and Authentication for Revocation Requests

Requests for certification revocation requests:

1. SHALL verify the identity and authority of the requestor;
2. SHALL provide the serial number;
3. SHALL provide the revocation reason;
4. SHALL authenticate the requestor and may use the public key of the certificate being revoked regardless of whether or not the private key has been compromised;
5. SHOULD provide the subject of the certificate; and
6. SHOULD provide the certificate’s validity period.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

A certificate application SHALL be submitted by one of the following requestors:

1. The subscriber;
2. An approved individual acting on behalf of the human subscriber or the organization;
3. A sponsor acting on behalf of non-human subscribers;
4. An RA acting on behalf of the subscriber; or
5. A CA.

4.1.2 Enrollment Process and Responsibilities

The following steps MAY be performed in any order that does not compromise security and MUST be completed before certificate issuance:

1. SHALL authenticate the requestor using credentials whose level of assurance is commensurate with the strength of the PKI;
2. SHALL protect the submitted information and key pair from modification;
3. SHALL protect the confidentiality of shared secrets and personally identifiable information;
4. SHALL ensure the requestor is authorized to submit certificate application requests;
5. SHALL ensure the requestor agrees to be bound by a relevant Subscriber Agreement that contains representations and warranties;
6. SHALL gather information to generate the certificate; and
7. SHALL validate the data provided.

4.2 Certificate Application Processing

The procedure for processing certificate applications:

1. SHALL verify PKCS#10 certificate requests conform with RFC 2986;
2. SHALL verify the accuracy of certificate applications;
3. SHALL ensure the authenticity of the requestor;
4. SHALL obtain any required approvals;
5. SHALL complete within 30 days from the time of certificate application submittal is posted on the CA or RA system;
6. SHALL NOT process any unverified certificate applications;
7. SHALL NOT process any certificate application that will reduce the overall level of assurance;
8. SHALL NOT process any rejected certificate applications;
9. SHOULD ensure that every certificate signed by the CA has a corresponding request in the RA; and
10. SHOULD provide the reason for rejection to the requestor.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

Upon receiving a request for an approved certificate, the CA:

1. SHALL authenticate the RA using credentials whose level of assurance is commensurate with the strength of the PKI;
2. SHALL ensure the RA is authorized to submit certificate application requests;
3. SHALL verify the integrity of the information in the certificate request;
4. SHALL check to ensure that all required fields and extension are properly populated;
5. SHALL ensure that the validity period of subscriber certificates does not exceed the issuing CA's validity period;
6. SHALL sign and issue a certificate if all certificate requirements have been met; and
7. SHALL provide the certificate to the requestor.

4.3.2 Notifications to Subscribers of Certificate Issuance

CAs or a representative acting on its behalf:

1. SHOULD inform the requestor of the certificate issuance; and
2. SHOULD instruct the requestor how to obtain the certificate.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Certificates SHALL be considered accepted if at least one of the following occurs prior to use:

1. The requestor fails to object to the certificate or its contents;
2. The requestor takes possession of the certificate; and
3. If an authorized agent of an organization formally accepts the certificate.

4.4.2 Publication of the Certificate by the CA

Certificates SHALL be published to repositories as necessary by the CA or a representative acting on its behalf.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

The CA or a representative acting on its behalf:

1. SHALL notify the RA of certificate issuance;
2. SHALL notify the Boeing PKI Policy Authority Board of root certificate issuance;
3. SHALL notify the Boeing PKI Policy Authority Board of cross-certificate issuance;
4. SHALL notify the authorized agent of an organization of cross-certificate issuance; and
5. MAY provide notification of end entity certificate issuance.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Responsibilities Relating to Their Private Key and Certificate Usage

Subscribers:

1. SHALL protect their private key from compromise (e.g., disclosure, tampering), unauthorized access, or unauthorized activation;
2. SHALL use private keys as intended in an applicable certificate profile as constrained by the attributes (e.g., key usage, extended key usage, certificate policies);
3. SHALL NOT use a certificate that is expired or has been revoked; and

4. SHOULD maintain certificates as required to support intended use (e.g., per a certificate profile document [Intended Use, Business Rules] or Subscriber Agreement).

4.5.2 Relying Party Responsibilities Relating to Use of a Subscriber's Private Key and Certificate

Relying parties:

1. SHALL validate the certificate;
2. SHALL validate the certificate chain;
3. SHALL use certificates for the purposes as described in an applicable certificate profile; and
4. SHALL NOT use a certificate that is expired or has been revoked.

4.6 Certificate Renewal

Renewing a certificate means creating a new certificate with the same name, key, and other information as the old one, but with a new, extended validity period and a new serial number.

4.6.1 Circumstance for Certificate Renewal

Certificates MAY be renewed if all of the following criteria are satisfied:

1. The certificate is allowed to be renewed;
2. All certificate attributes, other than the validity period and serial number, are left unchanged;
3. The information to be included in the certificate is verified to still be accurate;
4. The associated private key has not been revoked or compromised;
5. The certificate has not reached the end of its validity period; and
6. The validity period of the certificate does not exceed the remaining lifetime of the CA's certificate.

4.6.2 Who May Request a Certificate Renewal

Certificate renewal requests SHALL be submitted by one of the following requestors:

1. A subscriber;
2. An approved individual acting on behalf of the subscriber or the organization;
3. An RA acting on behalf of the subscriber; or
4. A CA.

4.6.3 Procedure for Processing Certificate Renewal Requests

The following steps MAY be performed in any order that does not compromise security and MUST be completed before submitting the certificate renewal request. The procedure:

1. SHALL confirm certificate satisfies the circumstances for renewal;
2. SHALL authenticate the requestor using credentials whose level of assurance is commensurate with the strength of the PKI;
3. SHALL protect the submitted information and key pair from modification;
4. SHALL protect the confidentiality of shared secrets and personally identifiable information;
5. SHALL ensure the requestor is authorized to submit certificate renewal requests;
6. SHALL ensure the requestor agrees to be bound by a relevant Subscriber Agreement; and
7. SHALL reuse the existing key pair of the certificate.

The procedure for processing certificate renewals:

8. SHALL verify the accuracy of certificate renewal request;
9. SHALL verify all certificate attributes, other than the validity period and serial number, are unchanged;
10. SHALL ensure the authenticity of the requestor;
11. SHALL obtain any required approvals;
12. SHALL complete the procedure within 30 days from the time of certificate renewal request submittal;
13. SHALL NOT process any unverified certificate renewal request;
14. SHALL NOT process any certificate renewal request that will reduce the overall level of assurance;
15. SHALL NOT process any rejected certificate renewal request; and
16. SHOULD provide the reason for rejection to the requestor.

Upon receiving a request for an approved renewal, the CA:

17. SHALL authenticate the requestor using credentials whose level of assurance is commensurate with the strength of the PKI;
18. SHALL ensure the requestor is authorized to submit certificate application requests;
19. SHALL verify the integrity of the information in the certificate request;
20. SHALL check to ensure that all required fields and extension are properly populated;
21. SHALL sign and issue a certificate if all certificate requirements have been met;
22. SHALL provide the certificate to the requestor; and
23. SHOULD revoke the old certificate.

4.6.4 Notification of New Certificate Issuance to Subscriber

A CA or a representative acting on its behalf:

1. SHOULD inform the subscriber of a certificate upcoming for renewal;
2. SHOULD inform the requestor of the certificate issuance; and
3. SHOULD instruct the requestor how to obtain the certificate.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Certificates SHALL be considered accepted if at least one of the following occurs prior to use:

1. The requestor fails to object to the certificate or its contents;
2. The requestor takes possession of the certificate; or
3. If an authorized agent of an organization formally accepts the certificate.

4.6.6 Publication of the Renewal Certificate by the CA

The CA or a representative acting on its behalf SHALL publish appropriate certificates to repositories as necessary.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

The CA or a representative acting on its behalf:

1. SHALL notify the RA of certificate issuance;
2. SHALL notify the Boeing PKI Policy Authority Board of root certificate issuance;
3. SHALL notify the Boeing PKI Policy Authority Board of cross-certificate issuance; and
4. SHALL notify the authorized agent of an organization of cross-certificate issuance.

4.7 Certificate Re-key

The longer and more often a key is used, the more susceptible it is to loss or discovery. Therefore, it is important that new keys are generated periodically.

Re-keying a certificate means creating a new certificate with the same name and other information as the old certificate, but with a new serial number and a new public key corresponding to a new private key.

4.7.1 Circumstance for Certificate Re-Key

Certificates MAY be re-keyed if all of the following criteria are satisfied:

1. The certificate is allowed to be re-keyed;
2. All certificate attributes are left unchanged other than the keys, serial number, and possibly the validity period;
3. Information to be included in the certificate is verified to still be accurate;
4. The certificate has not reached the end of its validity period;
5. The validity period of the certificate does not exceed the remaining lifetime of the CA's certificate; and
6. A valid MOA whose term covers the lifetime of the certificate MUST exist between Boeing and applicable third parties.

4.7.2 Who May Request Certificate Re-Key

Certificate re-key requests SHALL be submitted by one of the following requestors:

1. A subscriber;
2. An approved individual acting on behalf of the subscriber or organization;
3. A sponsor acting on behalf of non-human subscriber;
4. An RA acting on behalf of the subscriber; or
5. A CA.

4.7.3 CA and/or RA Procedure for Processing Certificate Re-Key Request

The following steps MAY be performed in any order that does not compromise security and MUST be completed before submitting the certificate re-key request. The procedure:

1. SHALL confirm certificate satisfies the circumstances for rekey;
2. SHALL authenticate the requestor using credentials whose level of assurance is commensurate with the strength of the PKI;
3. SHALL protect the submitted information and key pair from modification;
4. SHALL protect the confidentiality of shared secrets and personally identifiable information;
5. SHALL ensure the requestor is authorized to submit certificate re-key requests; and
6. SHALL ensure the requestor agrees to be bound by a relevant Subscriber Agreement that contains representations and warranties.

The procedure for processing certificate re-keys:

7. SHALL complete the procedure within 30 days from the time of certificate re-key request submittal;
8. SHALL verify the accuracy of certificate re-key request;

9. SHALL verify all certificate attributes are left unchanged other than the keys, serial number, and possibly the validity period;
10. SHALL ensure the authenticity of the requestor;
11. SHALL obtain any required approvals;
12. SHALL NOT process any unverified certificate re-key request;
13. SHALL NOT process any certificate re-key request that will reduce the overall level of assurance;
14. SHALL NOT process any rejected certificate re-key request; and
15. SHOULD provide the reason for rejection to the requestor.

Upon receiving a request for an approved re-key, the CA:

16. SHALL authenticate the requestor using credentials whose level of assurance is commensurate with the strength of the PKI;
17. SHALL ensure the requestor is authorized to submit certificate re-key requests;
18. SHALL verify the integrity of the information in the certificate re-key request;
19. SHALL check to ensure that all required fields and extension are properly populated;
20. SHALL sign and issue a certificate if all certificate requirements have been met;
21. SHALL provide the certificate to the requestor; and
22. SHOULD revoke the old certificate.

4.7.4 Notification of New Certificate Issuance to Subscriber

A CA or a representative acting on its behalf:

1. SHALL inform the requestor of the certificate issuance; and
2. SHOULD instruct the requestor how to obtain the certificate.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

Certificates SHALL be considered accepted if at least one of the following occurs prior to use:

1. The requestor fails to object to the certificate or its contents;
2. The requestor takes possession of the certificate; or
3. If an authorized agent of an organization formally accepts the certificate.

4.7.6 Publication of the Re-keyed Certificate by the CA

The CA or a representative acting on its behalf SHALL publish appropriate certificates to repositories as necessary.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

The CA or a representative acting on its behalf:

1. SHALL notify the RA of certificate issuance;
2. SHALL notify the Boeing PKI Policy Authority Board of root certificate issuance;
3. SHALL notify the Boeing PKI Policy Authority Board of cross-certificate issuance; and
4. SHALL notify the authorized agent of an organization of cross-certificate issuance.

4.8 Certificate Modification

Modifying a certificate means creating a new certificate that has the same key, a different serial number, and that differs in one or more other attributes (e.g., subject name, e-mail address, non-human sponsor) from the old certificate.

Because of the requirement to validate particular attribute changes, certificate modification is not allowed. Instead a new certificate would be obtained and the old certificate SHOULD be revoked.

4.8.1 Circumstance for Certificate Modification
Not applicable.

4.8.2 Who may request Certificate Modification
Not applicable.

4.8.3 CA and/or RA Procedure for Processing Certificate Modification Request
Not applicable.

4.8.4 Notification of New Certificate Issuance to Subscriber
Not applicable.

4.8.5 Conduct Constituting Acceptance of Modified Certificate
Not applicable.

4.8.6 Publication of the Modified Certificate by the CA
Not applicable.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities
Not applicable.

4.9 Certificate Revocation and Suspension
Certificate revocation and suspension renders the certificate unusable. Certificate suspension renders the certificate temporarily unusable whereas revocation does so permanently.

4.9.1 Circumstances for Certificate Revocation
Certificates and any derivative certificates issued SHALL be revoked or assessed for integrity and possible revocation if at least one of the following criteria are satisfied:

1. A certificate no longer represents the subject as described in the certificate profile;
2. A subscriber's employment is terminated or subscriber is suspended for cause;
3. A subscriber or subscriber's sponsor can be shown to have violated the stipulations of its Subscriber Agreement or certificate profile document;
4. A private key is compromised;
5. A private key is suspected of compromise and the security risk associated with leaving the certificate in place warrants revocation;
6. A subscriber or other authorized personnel asks for a certificate to be revoked;
7. A compromised certificate was used to sign a certificate request; or
8. A system failure results in loss of synchronization between an RA and the CA.

4.9.2 Who can Request Revocation of a Certificate
Certificate revocation requests SHALL be submitted by one of the following requestors:

1. A subscriber;
2. An approved individual acting on behalf of the subscriber or organization;

3. The Boeing PKI Policy Authority Board;
4. The Boeing PKI Operational Authority;
5. A Sponsor acting on behalf of non-human subscriber;
6. An RA acting on behalf of the subscriber; or
7. A CA.

4.9.3 Procedure for Certificate Revocation Request

The following steps MAY be performed in any order that does not compromise security and MUST be completed before submitting the certificate revocation request. The procedure:

1. SHALL confirm the request satisfies the circumstances for revocation;
2. SHALL identify the certificate to be revoked;
3. SHALL authenticate the requestor using credentials whose level of assurance is commensurate with the assurance level of the CA;
4. SHALL protect the submitted information from modification;
5. SHALL protect the confidentiality of shared secrets and personally identifiable information;
6. SHALL ensure the requestor is authorized to submit certificate revocation requests;
7. SHALL capture a brief explanation regarding the reason for the revocation; and
8. MAY request information sufficient to explain the reason for revocation.

The procedure for processing certificate revocations:

9. SHALL verify the accuracy of certificate revocation request;
10. SHALL ensure the authenticity of the requestor;
11. SHALL obtain any required approvals;
12. SHALL complete the procedure within 30 days from the time of certificate revocation request submittal;
13. SHALL NOT process any unverified certificate revocation request;
14. SHALL NOT process any rejected certificate revocation request; and
15. SHOULD provide the reason for rejection to the requestor.

Upon receiving a request for an approved revocation, the CA:

16. SHALL authenticate the requestor using credentials whose level of assurance is commensurate with the strength of the PKI;
17. SHALL ensure the requestor is authorized to submit certificate application requests;
18. SHALL verify the integrity of the information in the certificate request;
19. SHALL revoke the certificates after all revocation requirements have been met;
20. SHALL notify the subject of the revocation; and
21. SHALL publish the revocation status.

4.9.4 Revocation Request Grace Period

There is no revocation grace period.

4.9.5 Time within which CA Must Process the Revocation Request

Upon receiving an approved request for revocation, the CA SHALL process all revocation requests within the following prescribed time frame.

Assurance Level	Processing Time for Revocation Requests

Basic (hardware, software)	Within three days
Medium	Within six hours

4.9.6 Mechanism Used to Check Status of Certificates

Use of a revoked certificate could have damaging or catastrophic consequences. Mechanisms used to check status of certificates:

1. SHALL use either a published CRL or Certificate Status Authority (CSA) for Relying Parties to check certificate status; and
2. SHALL necessitate Relying Parties use at their discretion scalability testing for long CRLs impacting performance.

4.9.7 CRL Issuance Frequency

CRLs SHOULD be updated frequently, even if there are no changes made, without placing undue burden on the CAs, the certificate status services, and Relying Parties.

1. Online CAs that issue CRLs SHALL issue them at least once every 24 hours;
2. Offline CAs that issue:
    a. Basic assurance CRLs SHALL issue CRLs at least once every three months;
    b. Medium assurance CRLs SHALL issue CRLs at least once every month; and
3. CRLs SHALL ensure that the nextUpdate time provides sufficient buffer in the event that CRL publishing is delayed.

4.9.8 Maximum Latency for CRLs

Certificate status information:

1. SHALL be published no later than the next scheduled update; and
2. SHALL NOT exceed 4 hours from the time between CRL generation and publication.

4.9.9 On-line Revocation/Status Checking Availability

Online revocation/status checking availability:

1. SHALL be available for Relying Parties with access to the internet; and
2. SHALL meet or exceed the requirements for CRL issuance as specified elsewhere in this CP.

4.9.10 On-line Revocation/Status Checking Requirements for Relying Parties

Relying Parties:

1. SHALL NOT be required to use a certificate status service as long as a CRL is published on the PKI Repository or published via an out-of-band process; but
2. SHOULD do so in accordance with RFC 6960 if utilizing a certificate status service (e.g., OCSP).

4.9.11 Other Forms of Revocation Advertisements Available

Any alternate forms used to disseminate revocation information SHALL be implemented in a manner consistent with the security and latency requirements for the implementation of CRLs and on-line revocation and status checking.

4.9.12 Variations of Suspension/Revocations Assertions as a Result of Key Compromise

In the event of key compromise CRLs:

1. SHALL be published within 18 hours in the event of a lost or compromised private key; and
2. SHOULD be published immediately in the event of a revocation of a certificate with lost or compromised private key.

4.9.13 Circumstances for Certificate Suspension

Certificate suspension SHALL NOT be allowed.

4.9.14 Who Can Request Certificate Suspension

Not applicable.

4.9.15 Procedure for Certificate Suspension Request

Not applicable.

4.9.16 Limits on Certificate Suspension Period

Not applicable.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Revocation entries on a CRL or OCSP Response SHALL NOT be removed until after the Expiry Date of the revoked certificate.

4.10.2 Service Availability

Certificate Status Services SHALL be disaster tolerant so that any failure is transparent to the user.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

The certificate subscription is the period of time for which the certificate is valid. The subscription period SHALL end if at least one of the following criteria are satisfied:

1. The certificate is expired;
2. The certificate is revoked;
3. The certificate chain is no longer trusted; or
4. The service is terminated.

The end of certificate subscription:

5. SHALL trigger the revocation of CA certificates; and
6. SHOULD trigger the revocation of subscriber certificates.

4.12 Key Escrow and Recovery

Key escrow allows the CA or RA to retain a copy of a private key so that, under certain circumstances, an authorized party may recover the private key and use of the key.

4.12.1 Key Escrow and Recovery Policy and Practice Documentation Identification

A Key Recovery Practice Statement (KRPS) SHALL be developed if private keys can be escrowed and recovered.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices Documentation Identification

A KRPS SHALL be developed if session keys are used and can be recovered.

5. Management, Operational, and Physical Controls

5.1 Physical Security Controls

5.1.1 Site Location and Construction

Site location and construction is the first line of protection against unauthorized access designed.

Equipment used for CAs, cryptographic modules, CSAs, network equipment, PKI repositories, RAs and related databases:

1. SHALL be located in a Boeing-approved site (e.g., data center, cross-sites); and
2. SHALL use a physical barrier to separate medium level of assurance environments from lower level of assurance environments for online equipment.

Trusted workstations (used by medium assurance Trusted Agents and BCAP Trusted Agents), kiosks, and supporting peripherals:

3. SHALL be in the custody of the approved trusted role and under their physical control; and
4. SHALL be located in a Boeing facility approved by the Boeing PKI Operational Authority when used by MAH Trusted Agents.

Trusted Workstations (used by Badge Operators, Enterprise Help Desk, and Executive End User Support personnel, etc.):

5. SHALL be in the custody of the authorized personnel and under their physical control; and
6. SHALL be located in a Boeing facility approved by the Boeing PKI Operational Authority.

Administration Workstations and supporting peripherals:

7. SHALL be located in Boeing-approved work locations when used to administer basic assurance environments; and
8. SHALL be located in a Boeing-approved building (e.g., data centers, cross-sites) authorized by the Boeing PKI Operational Authority or The Boeing Company when used to administer medium level of assurance environments (including basic assurance hardware).

Security containers:

9. SHALL be either safes and/or lockable containers to secure material at a level that is commensurate with the sensitivity of the material as stipulated in the applicable CPS;
10. SHALL be provided to secure cryptographic module activation data that is not assigned to specific authorized trusted roles, sensitive materials, and smaller equipment; and
11. SHALL be located in a Boeing-approved building (e.g., data centers, cross-sites) authorized by the Boeing PKI Operational Authority or The Boeing Company.

5.1.2 Physical Access

Physical access controls:

1. SHALL grant physical access to Boeing PKI Operational Authority-authorized personnel;
2. SHALL prevent unauthorized physical access with increasing layers of security applied, such as perimeter, building, interior equipment room, and racks;
3. SHALL protect physical materials at a level that is commensurate with the sensitivity of the data;

4. SHALL prevent the theft of equipment; and
5. SHALL prevent tampering with equipment, whether accidental or malicious.

Additional physical access controls required for equipment located in Boeing-approved buildings (e.g., data centers or cross-sites) authorized by the Boeing PKI Operational Authority or The Boeing Company:

6. SHALL require escorts for non-authorized personnel;
7. SHALL monitor and detect physical access to the equipment;
8. SHALL record physical entry/access and exit/closure; and
9. SHALL ensure cryptographic modules are stored separately from the mechanism used to activate the module.

5.1.3 Power and Air Conditioning

Boeing data centers:

1. SHALL have backup power capability sufficient to lock out input, finish any pending actions, and record the state of the equipment automatically before lack of power causes a shutdown; and
2. SHALL have air conditioning capabilities sufficient to lock out input, finish any pending actions, and record the state of the equipment automatically before over heated equipment causes a shutdown.

Cross-sites SHALL have power and air conditioning capabilities sufficient to sustain equipment.

5.1.4 Water Exposure

Boeing equipment SHALL be installed such that it is not in danger of exposure to water excluding potential water damage from fire prevention and protection measures.

5.1.5 Fire Prevention and Protection

Boeing equipment SHALL be located in facilities that have fire prevention and protection adhering to out-of-band Boeing company policies and procedures.

5.1.6 Media Storage

Media SHALL be stored in a manner compliant with the requirements for the sensitivity level of the information to protect it from accidental damage, theft, and unauthorized physical access.

5.1.7 Waste Disposal

Physical materials (paper and media) containing sensitive information SHALL be disposed of in a secure manner to prevent accidental disclosure of the sensitive information. The disposal consists of, but is not be limited to, the following:

1. SHALL provide notification of destruction to the Boeing PKI OAA as part of CA termination or other major architecture changes (e.g., “a legacy environment completely refreshed”) as stipulated in an applicable CPS;
2. SHALL use Boeing-approved destruction containers (e.g., LIMITED destroy bins, shredders, *media* limited destroy bins, and Boeing company authorized HDD destruction containers);
3. SHALL adhere to manufacturers’ guidance (e.g., required for cryptographic modules) or NIST standards such as NIST SP 800-88);
4. SHALL be secured under same controls as it was in production until destroyed; and
5. SHALL adhere to stipulations in section 5.8 of this CP when applicable.

5.1.8 Off-Site Backup

The off-site backup SHALL use physical controls commensurate to the sensitivity of the data.

5.2 Procedural Controls

5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security or compliance problems if not carried out properly; regardless of whether the improper action was accidental or malicious. The personnel selected to fill trusted roles SHALL be trustworthy, demonstrate integrity and adhere to their assigned responsibilities or the integrity and trustworthiness of the PKI is weakened.

The security impact of trusted roles as they pertain to a specific assurance level is assessed. The trusted role risk assessment is an out-of-band process that ensures controls are applied sufficiently to reduce the likelihood of risk acceptable for the potential impact to the Business.

Required trusted role controls:

1. SHALL be determined based on trusted role risk assessment process results;
2. SHALL ensure the resulting risk rating associated with the trusted role is acceptable for the potential impact to the Business; and
3. SHALL be recorded for each trusted role in the applicable CPS.

Additionally, to further support the integrity and trustworthiness of the PKI, implementation of separation of duties and number of persons required per task may be required for trusted roles as defined elsewhere in this CP.

Persons responsible for at least one of the following PKI functions, including administering automated functions, SHALL be in a trusted role:

4. Install, configure, or maintain the operating systems of servers or systems performing CA, RA, and related databases functions;
5. Install, configure, or maintain the CAs, cryptographic modules, RAs, and related databases;
6. Install, configure, or maintain monitoring components;
7. Install, configure, or maintain network components;
8. Grant or revoke physical or logical access to the CAs, cryptographic modules, network equipment, RAs, and related databases equipment;
9. Access or manage security containers that contain materials supporting production services;
10. Access or manage cryptographic modules, their associated keying material, and the mechanism used to activate the module;
11. Approve, validate, authenticate, issue, revoke, or handle information in certificate requests, revocation requests, or renewal requests for critical certificates;
12. Verify identity of subscribers that do not have direct access to an RA or have a sponsor that does;
13. Approve key recovery requests and recover another subscriber’s keys;
14. Delete security or audit logs; or
15. Process audit logs and archive audit artifacts.

CAs that issue medium assurance or basic assurance hardware credentials have the following additional functions performed by trusted roles:

16. Install, configure, or maintain the operating systems of Trusted Workstations and Administration Workstations.

CAs that issue medium assurance credentials have the following additional functions performed by trusted roles:

17. Verify identity of subscribers for the required in-person or remote supervised identity vetting, as described elsewhere in this CP.

The following sections define the trusted roles.

5.2.1.1 Administrator

An Administrator MAY perform one or more of the following not to conflict with multi-person control or separation of duties as described elsewhere in this CP:

1. SHALL install, configure, or maintain PKI components;
2. SHALL install, configure, or maintain monitoring components;
3. SHALL install, configure, or maintain network components;
4. SHALL access or manage security containers that contain materials supporting production services;
5. SHALL approve, validate, authenticate, or handle information in certificate requests, revocation requests, or renewal requests;
6. SHALL issue or revoke certificates; or
7. SHALL delete security or audit Logs.

5.2.1.2 Audit Administrator

An Audit Administrator:

1. SHALL review (process) audit logs and other relevant activities;
2. SHALL investigate anomalies;
3. SHALL provide audit reports;
4. SHALL maintain audit logs of record; and
5. SHALL archive audit logs.

5.2.1.3 Certificate Manager (CM)

A Certificate Manager with Boeing PKI OAA approval:

1. SHALL approve enablement/disablement of certificate templates;
2. SHALL manage the issuance and revocation of critical certificates; and
3. SHALL approve certificate profiles.

5.2.1.4 Key Recovery Requestor (KRR)

This role recovers private keys in response to an approved key recovery request. A Key Recovery Requestor (KRR):

1. SHALL recover a subscriber's escrowed private key in response to an approved key recovery request;
2. SHALL provide private key to subscribers as appropriate; and
3. SHALL protect the recovered private key at a level commensurate with the private key when it was issued.

5.2.1.5 Key Recovery Officer (KRO)

This role reviews and approves key recovery requests. A Key Recovery Officer (KRO):

1. SHALL verify the authenticity and validity of key recovery request; and
2. SHALL approve or rejects a request to recover a subscriber's escrowed private key.

5.2.1.6 Trusted Agent (TA)

A Trusted Agent (TA):

1. SHALL submit requests for certificate application, renewal, and revocation on behalf of subscribers;
2. SHALL support certificate issuance;
3. SHALL validate the subscribers' identity;
4. MAY validate and submit CSRs to the RA on behalf of subscribers; and
5. MAY accept certificates on behalf of subscribers.

5.2.2 Number of Persons Required Per Task

Multi-person controls are used in situations where number of persons required per task and role separation cannot sufficiently reduce risk applicable to potential impact to the business. Additional multi-person control requirements for PCA/Root and Subordinate/Signing private signing keys are described in section 6.2.2 of this CP. Where multi-person control is required:

1. All personnel SHALL be in a trusted role;
2. One of the trusted roles SHALL be an administrator; and
3. It SHALL NOT be achieved using an Audit Administrator or Trusted Agent.

Multi-person controls are required for the activities listed below:

4. Accessing or configuring cryptographic modules including CA signing key generation and activation;
5. Managing cryptographic key protections;
6. Obtaining materials stored within safes; and
7. Deleting audit logs.

CAs that issue medium assurance and basic assurance hardware credentials have the following additional requirements:

8. Obtaining physical access to the equipment; and
9. Archiving audit evidence.

All trusted roles are recommended to have multiple persons serving in the trusted role in order to support continuity of operations.

5.2.3 Identification and Authentication of Trusted Role

An individual in a trusted role:

1. SHALL identify and authenticate before being permitted to perform any actions set forth above for that role or identity;
2. SHALL authenticate to remote components of the PKI using a credential that is commensurate with the strength of the PKI;
3. SHALL use an account for offline CAs that is local to the specific offline CA;
4. SHALL use a minimum of two factor authentication for online CAs and RAs, where at least one factor is a hardware token (using a method commensurate with or higher than the strength of the PKI); and
5. SHALL NOT be assigned more than one identity.

5.2.4 Roles Requiring Separation of Duties

Trusted roles requiring separation of duties:

1. SHALL NOT permit individuals who assume a Certificate Manager trusted role to serve in an administrator role within the same environment (e.g., MAH, BAH, BAS [including BCAP]);
2. SHALL NOT permit individuals who assume a Certificate Manager trusted role to serve in an Audit Administrator role;
3. SHALL NOT permit individuals who assume an Audit Administrator role to serve in any other trusted role; and
4. SHALL NOT permit any trusted roles to perform the Compliance Auditor function.

The Boeing PKI OAA:

5. SHALL define and record the appropriate separation of duty restrictions for other trusted roles in an applicable CPS; and
6. SHALL ensure other trusted role risk assessments performed are assessed applicably for potential impact to the business.

5.3 Personnel Controls

5.3.1 Qualification, Experience, and Clearance Requirements

Qualified personnel serving in trusted roles are essential to the security and correct operation of the PKI.

All personnel filling a trusted role:

1. SHALL satisfy employment requirements required for the strength of the PKI:
    a. CAs that issue medium assurance and basic assurance hardware credentials – Boeing direct hire;
    b. CAs that issue basic assurance software – Boeing direct hire or non-Boeing personnel as defined in the applicable CPS based upon the trusted role risk assessments acceptable for the potential impact to the Business;
2. SHALL be a citizen of the country allowed or U.S. Person required for the strength of the PKI:
    c. CAs that issue medium assurance and basic assurance hardware credentials – a U.S. citizen for all trusted roles excluding medium assurance Trusted Agents; medium assurance Trusted Agents – a citizen of the country where the Trusted Agent role is performed;

d. CAs that issue basic assurance software – a U.S. citizen or U.S. person (per Boeing company policy definition).

3. SHALL be appointed in writing or electronically by an approving authority;
4. SHALL be verified periodically for continued need and terminated from the trusted role if no longer needed;
5. SHALL favorably complete a background investigation;
6. SHALL NOT have had a security clearance revoked for reasons other than routine review and renewal decisions;
7. SHALL NOT have been denied a security clearance, the cause for which has not been resolved, and either have had a security clearance subsequently granted or they have cleared a separate (i.e., not part of security clearance) enhanced background screening;
8. SHALL NOT be given access to production until:
   e. Favorably completing a background investigation;
   f. Providing signed trusted roles training acknowledgements; and
   g. Providing signed trusted role responsibility acknowledgements.

   CAs that issue medium assurance and basic assurance hardware credentials have the following additional production access requirement for trusted roles:
   h. Satisfying their manager's six-month verification if they are a new Boeing employee.
9. SHALL NOT have other duties that would conflict with their duties for the trusted role;
10. SHALL NOT have been previously relieved of duties resulting from violation of trust (e.g., willful mishandling of information or willful mis-issuance or revocation of certificates); and
11. SHALL NOT have been criminally convicted (as legally reportable) as pre-determined by the Boeing review/adjudication team criteria.

CAs that issue medium assurance credentials have the following additional requirements for Trusted Agents:

12. SHALL favorably complete a background screening from obtaining a security clearance equivalent to U.S. Secret or higher issued by a NATO member nation or major NATO ally as defined by the International Traffic in Arms Regulation (ITAR) – 22 CFR 120.32.

To be considered valid, a security clearance:

13. SHALL be issued by a NATO member nation or major non-NATO ally as defined by the International Traffic in Arms Regulation (ITAR) – 22 CFR 120.32.

5.3.2 Background Check and Clearance Procedures

Background checks and clearances are used to identify any activity that could render personnel untrustworthy or susceptible to compromise.

Background checks for all trusted roles *excluding* medium assurance Trusted Agents:

1. SHALL use the Boeing Internal Data Protection (IDP) enhanced background screening process or equivalent (which may be a combination of an IDP enhanced background screening, and/or company hire-in background screenings, etc.);
2. SHALL ensure adjudication (i.e., final determination) process is consistent with out-of-band Boeing company policies and procedures; and
3. SHALL be refreshed per out-of-band Boeing company policies and procedures.

Background checks for medium assurance Trusted Agents:

4. SHALL be per process to obtain a security clearance equivalent to U.S. Secret or higher issued by a NATO member nation or major NATO ally as defined by the International Traffic in Arms Regulation (ITAR) – 22 CFR 120.32; and
5. SHALL be refreshed as dictated by a security clearance.

At a minimum, the scope of a background check:

6. SHALL include employment for the past five (5) years;
7. SHALL include the highest post-secondary educational degree earned regardless of award date;
8. SHALL include residence for the past three (3) years; and
9. SHALL include law enforcement (i.e., criminal conviction history [as legally reportable]) for the past five (5) years.

CAs that issue medium assurance and basic assurance hardware credentials have the following additional background check requirement for trusted roles:

10. SHALL include references.

5.3.3 Training Requirements and Procedures

Training ensures that personnel are properly equipped to carry out the duties for the assigned trusted roles.

All personnel filling a trusted role:

1. SHALL receive training on PKI Governance;
2. SHALL receive training on the expectations and duties of the trusted role;
3. SHALL receive training on all applicable security principles and mechanisms for the trusted role;
4. SHALL receive training on all applicable practices and procedures for the trusted role;
5. SHALL have demonstrated the ability to perform their duties;
6. SHALL accept and acknowledge the training and responsibilities of their trusted role;
7. SHALL receive ethics training per Boeing policy; and
8. SHALL receive training on incident and compromise reporting.

5.3.4 Retraining Frequency and Procedures

All personnel filling a trusted role:

1. SHALL be made aware of any changes to operations;
2. SHALL be made aware of changes to all applicable practices or procedures;
3. SHALL accept and acknowledge the retraining and responsibilities of their trusted role; and
4. SHOULD receive training to refresh the existing knowledge of security principles, practices, procedures, and trusted role duties on a yearly basis.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

Unauthorized actions will not be tolerated. Personnel who violate this policy SHALL receive appropriate administrative or disciplinary actions.

5.3.7 Independent Contractor Requirements

Non-Boeing personnel SHALL satisfy all applicable requirements set forth in this CP.

5.3.8 Documentation Supplied to Personnel

All personnel filling a trusted role:

1. SHALL have access to this certificate policy; and
2. SHALL have access to all documentation necessary to perform the duties of the trusted role.

5.4 Audit Logging Procedures

Audit logging procedures report on operations performed in the environment. Audit log procedures:

1. SHALL prove operations comply with policy;
2. SHALL verify security of the environment;
3. SHALL ensure configuration is managed;
4. SHALL include processing (reviewing) and reporting to the Boeing PKI OAA; and
5. SHALL ensure all anomalous events are analyzed to determine cause with supporting resolutions resulting in items 1 – 3 above being fulfilled.

5.4.1 Types of Events Recorded

Types of events SHALL be recorded for all PKI, monitoring and network components which:

1. SHALL include the type of event;
2. SHALL contain the date and time of occurrence;
3. SHALL include the appropriate status (e.g., success or failure);
4. SHALL identify the originator of the event or transaction;
5. SHALL include a description of the event;
6. SHALL include a statistically significant sampling of audit data;
7. SHALL specify specific auditable events in a CPS;
8. SHOULD be electronically system-generated; and
9. MAY be manually created when electronic means do not exist.

5.4.2 Frequency of Processing Audit Logs

Audit logs:

1. SHALL be reviewed monthly for online components;
2. SHALL be reviewed when the offline component is activated; and
3. SHALL be reviewed whenever deemed necessary or warranted by an alarm or suspected anomalous event.

5.4.3 Retention Period for Audit Logs

Audit logs:

1. SHALL be maintained to support reviewing (processing) of the logs; and
2. SHALL be maintained to support Boeing company or regulatory requirements.

CAs that issue medium assurance credentials have the following additional requirement:

3. SHALL retain processed audit logs, which become audit logs of record, by Audit Administrators until archived as asserted elsewhere in this CP.

5.4.4 Protection of Audit Logs

Audit log controls:

1. SHALL restrict access to authorized personnel;
2. SHALL protect audit logs from unauthorized modifications;
3. SHALL detect tampering of audit logs;
4. SHALL protect audit logs from being overwritten or deleted until after the audit logs have been offloaded; and
5. SHALL ensure offloaded audit logs are protected in a manner equivalent to online audit logs.

5.4.5 Audit Log Backup Procedures

Audit logs:

1. SHALL be backed up at regularly scheduled intervals;
2. SHOULD be backed up more frequently for online components than offline components; and
3. MAY be backed up whenever deemed necessary or warranted.

5.4.6 Audit Log Collection System (Internal vs. External)

Audit logs MAY be collected by an external system.

5.4.7 Notification to Event-Causing Subject

Notifications SHALL NOT be sent to the event causing subject unless required by a Monitoring Plan.

5.4.8 Vulnerability Assessments

Vulnerability assessments SHALL be defined in section 8 of this CP, Security Assessments.

5.5 Records Archival

Records archival ensures that sufficient evidence is retained to prove compliance with PKI policies and practices.

5.5.1 Types of Records Archived

PKI, monitoring, and network components' archive records:

1. SHALL be sufficiently detailed to establish the proper operation of the PKI or the validity of any certificate (including those revoked or expired) issued by the CA;
2. SHALL include, but are not limited to, the following:
    a. Certificate Policy and Practice Statements;
    b. Cross-Certification or Trust Agreement documentation;
    c. Compliance records and reports;
    d. Internal audit reports;
    e. All electronic auditable data;
    f. Change requests;
3. SHALL be archived for medium assurance level artifacts; and
4. MAY be archived for basic assurance hardware and software per regulatory requirements or as otherwise deemed necessary.

5.5.2 Retention Period for Archive

Archive records:

1. SHALL be maintained to support retention requirements as defined in a records retention plan; and
2. SHALL be retained for 10 and half years for medium assurance level artifacts.

5.5.3 Protection of Archive

Protection of archive:

1. SHALL restrict access to authorized personnel;
2. SHALL prevent modification of the archive;
3. SHALL prevent unapproved overwriting or deletion of the archive;
4. SHALL ensure the viability of archive media is sufficient for the retention period;
5. SHALL ensure archive contents are readable during the retention period regardless of technology obsolescence;
6. SHOULD detect tampering of the archive; and
7. SHOULD be stored separately from where the archive content originated.

5.5.4 Archive Backup Procedures

No stipulation.

5.5.5 Requirements for Time Stamping Records

Archive records SHALL be time stamped as they are created.

5.5.6 Archive Collection System (Internal or External)

No stipulation.

5.5.7 Procedures to Obtain & Verify Archive Information

Obtaining and verifying archive information:

1. SHALL require Boeing PKI PA Chair or Boeing PKI OAA approval prior to archive retrieval; and
2. SHALL ensure compare the contents of the archive to a separately maintained manifest generated at the time of the archive creation.

5.6 Key Changeover

Key changeover procedures:

1. SHALL ensure affected entities are notified of the key changeover; and
2. SHALL post the change to the PKI Repository.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Reporting and Handling Procedures

An Incident and Compromise Management procedure is used to quickly assess and mitigate any events that could jeopardize the stability or security of the PKI environment.

An incident and compromise management procedure:

1. SHALL require incidents are reported to appropriate personnel;
2. SHALL include investigating all incidents;
3. SHALL document incident mitigations;
4. SHALL determine whether the incident led to a compromise;
5. SHALL communicate initial assessment of the compromise to appropriate personnel or external entities;
6. SHALL document compromise mitigations;
7. SHALL verify normal operations after mitigations are complete; and

8. SHALL communicate final disposition to appropriate personnel or external entities.

CAs that issue medium assurance credentials have the following additional requirements:

9. SHALL notify CertiPath within 24 hours of determining that an incident (related to sections 5.7.1, 5.7.2, and 5.7.3 in this CP) has occurred with the potential to affect the operations and/or security environments and provided a preliminary remediation analysis;
10. SHALL within 10 business days of incident resolution, post a notice on its public web page identifying the incident and notify CertiPath that the notice has been posted; and
11. SHALL include the following in the public notice:
    a. Which CA components were affected by the incident;
    b. The CA's interpretation of the incident;
    c. Who is impacted by the incident;
    d. When the incident was discovered; and
    e. A statement that the incident has been fully remediated.

5.7.2 Corrupted Computing Resources, Software and/or Data Recovery Procedures

Backups are used to recover systems or data that have failed or become corrupted. Backup procedures:

1. SHALL ensure all system components are backed up in a manner that is sufficient to recover from system failure or corruption (e.g., implementing disparate networks and/or having disconnected/offline backups);
2. SHALL ensure backups are created regularly;
3. SHALL ensure backups are protected at a level commensurate with the original systems or data;
4. SHALL ensure backups are stored onsite in order to recover from system failure; and
5. SHALL ensure backups are stored at an offsite location in a manner that is sufficient to recover from a site failure or disaster.

In the event that system or data have failed or become corrupted, recovery procedures:

6. SHALL reestablish operations as quickly as possible from backups;
7. SHALL give priority to revoking certificates;
8. SHALL give priority to generating certificate status information;
9. SHALL verify system and data integrity before returning to normal operations; and
10. SHOULD attempt to recover data lost since the last successful backup.

In the event that system or data recovery is not possible in a reasonable timeframe, the appropriate procedures:

11. SHALL determine whether to revoke previously issued certificates;
12. SHALL determine whether to issue a final CRL;
13. SHALL notify subscribers of any action required;
14. SHALL rebuild non-recoverable PKI, monitoring, and network components necessary to reestablish normal operations;
15. SHALL give priority to generating a new CA signing key pair; and
16. SHALL give priority to generating certificate status information.

5.7.3 Recovery Procedures when Entity Key Is Compromised

If entity keys are "suspected" or "known" to be compromised, the Boeing PKI Operational Authority:

1. SHALL immediately execute Boeing Incident and Compromise Management procedures;
2. SHALL establish a recovery plan consisting of, but not limited to:

a. Applying applicable assertions in section 5.7.2 of this CP;
b. Investigating private key impacts during which determination is made to revoke and/or destroy the key;
c. Requiring new certificate requests are made in accordance with the initial registration requirements described elsewhere in this CP;
d. Verifying the CA can obtain accurate information on the certificates it has issued and that are still valid (i.e., not expired or revoked) therefore allowing the CA to re-issue (i.e., renew) those certificates with the notAfter date in the certificate remaining the same as the original certificates;
e. Providing subscribers the new trust anchor if the CA is a PCA/Root CA via secure means ensuring trust anchor integrity (e.g., using TLS authentication);
f. Immediately revoking RA certificates if entity is an RA;
g. Verifying all certificate requests approved by the RA since the date of the suspected or confirmed compromise are reviewed to determine which are legitimate;
h. Revoking certificates for which their request or approval legitimacy cannot be obtained;
i. Notifying the subject of the revoked certificates of the revocation; and
j. Assessing CSA certificates and potential revocation.

5.7.4 Business Continuity Capabilities after a Disaster

In order to maintain business continuity of PKI services and systems in the event of a disaster, the Boeing PKI Operational Authority:

1. SHALL maintain detailed procedures that outline the steps required to recover from a site failure or disaster;
2. SHALL test Disaster Recovery Plans on regular basis;
3. SHALL ensure backups are available at an offsite location in a manner that is sufficient to recover from a site failure or disaster;
4. SHALL have a secure location where operations can be restored in the event of a disaster at the primary location;
5. SHALL ensure availability of personnel to execute the Disaster Recovery Plan; and
6. SHALL execute Boeing company procedures for securing facilities during the period of time following a natural or other disaster and before a secure environment is re-established.

5.8 CA or RA Termination

In the event that it is necessary to terminate the operation of a Boeing CA or RA, the Boeing PKI OA:

1. SHALL provide as much advance notice, as circumstances permit, regarding CA or RA termination to appropriate personnel, subscribers, or external entities;
2. SHALL determine the appropriate actions to minimize the impact of CA or RA termination;
3. SHALL follow a documented termination ceremony;
4. SHALL preserve relevant records to support retention requirements;
5. SHALL prevent continued use of certificates;
6. SHALL follow hardware destruction processes (see section 5.1.7 of this CP);
7. SHALL destroy all keys (see section 6.2.10 of this CP) that are still available excluding keys required to retain key history (e.g., for encrypted email recovery);
8. SHALL communicate final disposition to appropriate personnel, subscribers, or external entities.
9. SHOULD issue and publish a final CRL prior to termination as stipulated in an applicable CPS; and
10. SHOULD issue a final OCSP signing certificate prior to termination as stipulated in an applicable CPS.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Key Pairs:

1. SHALL use FIPS 140-2 Level 3 certified hardware cryptographic modules for CA, RA, and CSA key pairs;
2. SHALL use either software or hardware at the same or higher assurance level of the CA to generate end entity key pairs;
3. SHALL use multi-person control as specified section 5.2.2 of this CP;
4. SHALL require a verifiable audit trail for CA key pair generation ensuring security controls are followed (detailed enough to show role separation was used) and approved by the Boeing PKI OAA;
5. SHALL destroy private keys after they have been transferred to the subscriber when the private key is not generated on the end entity (this does not prohibit the key generating module to act as the key escrow module);
6. SHALL NOT be exported outside any CA or RA unless encrypted;
7. SHALL NOT be exported outside any end entity device unless encrypted; and
8. SHOULD be generated by subscribers whenever possible.

CAs that issue medium assurance credentials have the following additional requirement:

9. SHALL require a third-party validation of the CA key pair generation.

CAs that issue medium assurance and basic assurance hardware credentials have the following additional requirements:

10. SHALL require multi-factor authentication via HSM operator cards by Trusted Roles for a CMS Master Key generation and installation;
11. SHALL require the keys are protected with an HSM for key diversification operations; and
12. SHALL require CMS Master Key and diversified keys are protected from unauthorized disclosure and distribution.

6.1.2 Private Key Delivery to Subscriber

In the event the subscriber does not generate the key pair, the method to deliver private keys:

1. SHALL ensure that the appropriate keys are provided to the correct subscribers or responsible personnel;
2. SHALL protect the private key from compromise or unauthorized activation using controls appropriate for the security level of the cryptographic module;
3. SHALL require the CA or RA maintain a record of the subscriber’s acknowledgment of receipt; and
4. SHALL ensure any additional copies of private keys are destroyed after delivery to the subscriber (this does not prohibit the key generating modules to act as the key escrow module also).

6.1.3 Public Key Delivery to Certificate Issuer

For public keys generated by the subscriber or RA, the method to deliver public keys to the CA:

1. SHALL ensure that transport is secure;
2. SHALL ensure the delivery mechanism binds the subscriber’s verified identity to the public key; and;
3. SHALL ensure cryptography, if used for the binding, is commensurate with the strength of the CA keys used to sign the certificate.

6.1.4 Public Key Delivery to Relying Parties

Provision of the public key for an Issuing CA SHALL be available by a secure protocol via the PKI Repository.

6.1.5 Key Sizes

All public keys placed in newly generated certificates (including self-signed certificates) and uses of public key cryptography by PKI components for signature and/or key agreement/encryption operations SHALL use one of the following algorithms for the time periods indicated:

Type	Public Key Algorithm	Sunset Date
Signature	2048 bit RSA, 224 bit ECDSA in prime field, or 233 bit ECDSA in binary field	12/31/2030
	3072 or 4096 bit RSA, 256 bit ECDSA in prime field, or 283 bit ECDSA in binary field	No stipulation
Encryption	2048 bit RSA, 224 bit ECDH in prime field, or 233 bit ECDH in binary field	12/31/2030
	3072 or 4096 bit RSA, 256 bit ECDH in prime field, or 283 bit ECDH in binary field	No stipulation

All data encryption (including network protocols) used by or in connection with PKI components for administration, communications, and protection of keys or other sensitive data SHALL use the following symmetric algorithms for the time periods indicated:

Type	Name	Sunset Date
Symmetric Algorithms	3 Key TDES	Deprecated. May be used until 12/31/2023 only for data blocks that are 8 MB or less per unique key bundle. 1
	AES	No stipulation

All certificates, CRLs, and OCSP Responses SHALL use one of the following hash algorithms for the time periods indicated:

Type	Issued before 12/31/2030	Issued after 12/31/2030
Hashing Algorithm for Certificates	SHA-224, SHA-256, or SHA-384	SHA-256
Hashing Algorithm for CRLs	SHA-224, SHA-256, or SHA-384	SHA-256
Hashing Algorithm for OCSP Responses	SHA-224, SHA-256, or SHA-384	SHA-256

CRLs, OCSP Responder certificates, and OCSP Responses:

1. SHALL use the same or stronger signature algorithms, key sizes, and hash algorithms as used by the CA to sign the certificate in question; and
2. MAY be signed using SHA-1 for CRLs and pre-signed OCSP responses for LEGACY Certification Authorities.

All PKI components that use hash algorithms for security relevant functions, such as key generation or agreement, communication protocols (e.g., Transport Layer Security [TLS]), or password protection, SHALL use the same or larger bit versions of the hash algorithm(s) used by the CA to sign certificates.

6.1.6 Parameters Generation and Quality Checking

RSA keys:

1. SHALL be generated in accordance with FIPS 186-4 for CAs and RAs;

[1] See NIST SP 800-131 regarding the deprecation of 3 Key TDES

2. SHALL be generated for subscribers at the medium assurance credentials in accordance with FIPS 186-4;
3. SHOULD be generated in accordance with FIPS 186-4 for subscribers at basic assurance level; and
4. SHOULD use prime numbers generated or tested for primality in accordance with FIPS 186-4.

6.1.7 Key Usage Purposes

The use of a key is specified in the key usage and extended key usage attributes for X.509 Version 3 certificates.

The key usage attribute:

1. SHALL assert only the digitalSignature bit for keys used solely for authentication;
2. SHALL assert the digitalSignature and *nonrepudiation* bits for keys used for digital signatures for CAs that issue medium and basic assurance hardware credentials;
3. SHALL assert the keyEncipherment bit for keys used for encryption;
4. SHALL assert the keyAgreement bit for keys used for key agreement;
5. SHALL assert the cRLSign and keyCertSign bits for keys by CAs;
6. SHALL NOT assert both the keyEncipherment and digitalSignature bits (this restriction is not intended to prohibit use of protocols like the Secure Socket Layer [SSL] / Transport Layer Security [TLS] that provide authenticated connections using key management certificates and require setting both digitalSignature and keyEncipherment bits);
7. SHALL NOT assert the keyEncipherment bit or keyAgreement bit when the nonrepudiation bit is set; and
8. SHOULD assert the digitalSignature and nonrepudiation bits for keys used for digital signatures for CAs that issue basic assurance software credentials.

End entity certificates have the following additional requirement for the Extended Key Usage extension:

9. SHALL always be present;
10. SHALL be consistent with the key usage bits asserted; and
11. SHALL NOT contain anyExtendedKeyUsage {2.5.29.37.0}.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards & Controls

Cryptographic modules:

1. SHALL use FIPS 140-2 Level 3 cryptographic modules for all levels of assurance for CAs, RAs, and CSAs under this CP; and
2. SHALL be commensurate with the CA's level of assurance for end entity subscribers' cryptographic modules.

Other comparable validation, certification, or verification standards:

3. SHALL ensure private keys protected by a cryptographic module do not exist outside the cryptographic module in plaintext form;
4. SHALL satisfy the intent of FIPS 140-2;
5. SHALL be approved by the Boeing PKI Policy Authority Board or Operational Authority Members' Group; and

6. SHALL be documented in this Certificate Policy.

6.2.2 Private Key Multi-Person Control

Private key multi-person control for PCA/Root and Subordinate/Issuing CA private signing keys:

1. SHALL require action by at least two persons in trusted roles as described section 5.2.2 of this CP; and
2. SHALL require HSM-enforced multi-person control.

6.2.3 Private Key Escrow

Escrowed private keys:

1. SHALL be recoverable only by authorized personnel;
2. SHALL be escrowed using security controls that are commensurate with the protection used to secure the original keys;
3. SHALL use escrowed keys only for the purpose of email encryption key history or recovery; and
4. SHALL NOT be retained by an external third party; and
5. SHOULD be escrowed when used for encryption unless the data protected by these keys will never require recovery.

6.2.4 Private Key Backup

Backups of private keys used by non-human subscribers:

1. SHALL be allowed for keys contained in software-based and hardware-based certificates in encrypted form;
2. SHALL be held in the controls of the non-human subscriber’s human sponsor or authorized personnel; and
3. SHALL be stored using security controls that are commensurate with the protection provided by the subscriber’s cryptographic module.

Backups of private keys used by human subscribers:

4. SHALL be allowed for keys contained in software-based certificates in encrypted form;
5. SHALL be held in the subscriber’s control;
6. SHALL be stored using security controls that are commensurate with the protection provided by the subscriber’s cryptographic module; and
7. SHALL NOT be allowed for keys contained in hardware-based certificates.

6.2.5 Private Key Archival

Archived private keys:

1. SHALL NOT be retained by an external third party;
2. SHALL be recoverable only by authorized personnel;
3. SHALL be protected using security controls that are commensurate with the protection used to secure the original keys; and
4. SHOULD be archived when used for encryption unless the data protected by these keys will never require recovery.

6.2.6 Private Key Transfer into or from a Cryptographic Module

Private keys for CAs, RAs, and CSAs:

1. SHALL be transferred by trusted roles defined elsewhere in this CP;
2. SHALL be protected during transport using security controls that are commensurate with the protection provided by the cryptographic module;
3. SHALL always be encrypted during transport;
4. SHALL NOT be transferred to a less secured cryptographic module; and
5. MAY be transferred to an equivalent or more secure cryptographic module.

6.2.7 Private Key Storage on Cryptographic Module

MAY store private keys in any form as long as the keys are not accessible without an authentication mechanism that complies with the cryptographic module standards defined elsewhere in this CP.

6.2.8 Method of Activating Private Keys

Private key activation:

1. SHALL require authentication by the authorized administrator only at CA, RA, or CSA start up;
2. SHALL require authentication by the subscriber for each operation;
3. SHALL satisfy the authentication requirements defined for the cryptographic module in FIPS 140-2; and
4. MAY be achieved for the use of cached authentication credentials provided that the cache is secured through the use of appropriate controls.

6.2.9 Method of Deactivating Private Keys

Private key deactivation:

1. SHALL be performed by trusted roles for CA, RA and CSA private keys as described elsewhere in this CP;
2. SHALL occur automatically once the CA or RA service is stopped; and
3. SHALL occur automatically once the subscriber-initiated operation is complete.

6.2.10 Method of Destroying Private Keys

Private key destruction:

1. SHALL occur when the private keys are no longer needed;
2. SHALL be accomplished using an approved manner as stipulated in an applicable CPS; and
3. SHOULD occur when the certificates to which they correspond expire or are revoked.

6.2.11 Cryptographic Module Rating

Cryptographic modules under this CP SHALL conform to FIPS 140-2.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

No stipulation.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The initial usage periods:

1. SHALL be defined in a certificate profile located in the PKI Repository; and
2. SHALL be approved by the Boeing PKI Operational Authority.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Activation data:

1. SHALL be used to activate CA, RA, and CSA private keys;
2. SHALL either entail the use of biometric data or meet the authentication requirements stipulated for the security level of the cryptographic module as described elsewhere in this CP;
3. SHALL be protected if transmitted via an appropriately protected channel and distinct in time and place from the associated cryptographic module;
4. SHALL have an appropriate level of strength for the keys or data to be protected;
5. SHALL be changed if the activation data is a password when a CA, RA, or CSA is re-keyed; and
6. SHOULD be generated by subscribers or authorized personnel whenever possible.

6.4.2 Activation Data Protection

Activation data:

1. SHALL ensure that the activation data is provided to the correct subscriber or authorized personnel;
2. SHALL protect the activation data from unauthorized disclosure using controls appropriate for the security level of the cryptographic module;
3. SHALL be securely stored separately from the cryptographic module or associated key;
4. SHALL be destroyed or decommissioned using methods that protect against unauthorized disclosure or use, modification, or unauthorized use of the private key protected by the activation data;
5. SHALL include a mechanism to temporarily lock the account, or terminate the application after pre-determined number of failed login attempts using the activation data; and
6. SHALL generate new security tokens (e.g., SecureBadge, Identity Smartcards, HSM cards) or be reset when activation data compromised.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

Computer security controls ensure PKI operations are performed as specified in this certificate policy and:

1. SHALL require authenticated logins before performing any actions using a method commensurate with the strength of the PKI;
2. SHALL provide Discretionary Access Control;
3. SHALL establish a trusted path prior to identification and authentication;
4. SHALL protect the confidentiality (encrypted or otherwise secured) and integrity (signed or otherwise maintained) of data (e.g., backups, configuration data) at rest;
5. SHALL prevent connections from PKI, monitoring, and network components from untrusted sources;
6. SHALL ensure the operating system prevents unauthorized changes;
7. SHALL ensure only necessary hardware and software is present on the system;

8. SHALL disable unnecessary listeners and services;
9. SHALL use system configurations that have been evaluated for compliance;
10. SHOULD ensure memory safe operations;
11. SHOULD use the same system configuration in non-production and production environments;
12. SHOULD use dedicated hardware and software; and
13. MAY allow remote logins for PKI, monitoring, and network components if it doesn't contradict other assertions in this CP.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life-Cycle Security Controls

6.6.1 System Development Controls

The System Development Controls for PKI, monitoring, and network components:

1. SHALL ensure change requests are formally approved and tracked to completion;
2. SHALL ensure the configuration of hardware and software is properly managed;
3. SHALL ensure solutions are securely designed, developed, tested, deployed, and maintained;
4. SHALL obtain approvals at key stages of the life-cycle including requirements specifications, design, development, user acceptance testing, and deployment; and
5. SHALL only use approved hardware and software from authorized sources.

6.6.2 Security Management Controls

The security management controls for PKI, monitoring, and network components:

1. SHALL provide monitoring and alerting, with auditing capability, that would detect disabling, modifying, or subverting security controls that maintain the integrity of a system;
2. SHALL establish monitoring and alerting, with auditing capability, of CA or other critical certificates or keys when issued or revoked;
3. SHALL detect and remediate suspected or confirmed malicious components;
4. SHALL confirm the integrity of the hardware and software; and
5. SHALL detect unauthorized modification to hardware and software.

6.6.3 Life-Cycle Security Ratings

No stipulation.

6.7 Network Security Controls

Network security controls for PKI, monitoring, and network components:

1. SHALL deny all but the necessary inbound and outbound network access;
2. SHALL protect the confidentiality and integrity of data in transit; and
3. SHALL implement protection against known network attacks.

6.8 Time-stamping

System time:

1. SHALL be synchronized with an approved atomic time-based source; and
2. SHALL be accurate within three minutes.

Timestamps derived from the atomic time-based source:

3. SHALL establish initial validity time of a subscriber’s certificate;
4. SHALL establish the time of revocation of a subscriber’s certificate;
5. SHALL establish the time of posting of CRL updates; and
6. SHALL establish the time of OCSP or other CSA responses.

7. Certificate and CRL Profiles

7.1 Certificate Profile

Certificate profiles:

1. SHALL be documented with specific certificate usage and attribute values;
2. SHALL be located on the PKI Repository in an approved certificate profile document; and
3. SHALL be reviewed at least annually and updates applied as required.

7.1.1 Version Numbers

The use of version numbers SHALL comply with the X.509 standard defined in RFC 5280.

7.1.2 Certificate Extensions

Certificate extensions for Issuer CA and subscriber certificates:

1. SHALL be marked critical=yes for required extensions;
2. SHALL be marked critical=no for optional extensions; and
3. MAY be included as specified by RFC 5280.

Certificate extensions for cross-certified certificates SHALL be marked *critical=yes* only if the intended relying parties have agreed to the use of the extension.

The CRL Distribution Points (CDP) extension:

4. SHALL provide a reference to certificate revocation information that is publicly available via an HTTP URL with the exception of OCSP Responder certificates that include the id-pkix-ocsp-nocheck extension; and
5. SHOULD appear only after the HTTP pointers if LDAP pointers are used.

The Authority Information Access (AIA) extension:

6. SHALL provide a reference to Certificate Status Authority and Certification Authority information that is publicly available; and
7. SHOULD provide LDAP pointers, if used, after the HTTP pointers.

7.1.3 Algorithm Object Identifiers

Certificates issued under this CP SHALL use the following OIDs for signatures:

Algorithm	OID
ecdsa-with-Sha 2	1.2.840.10045.4.3.2
sha-1WithRSAEncryption	1.2.840.113549.1.1.5
sha-2WithRSAEncryption	1.2.840.113549.1.1.11

Certificates under this CP SHALL use the following OID for identifying the subject public key information:

Algorithm	OID
id-ecdhPublicKey	1.3.132.1.12
id-ecPublicKey	1.2.840.10045.2.1
rSAEncryption	1.2.840.113549.1.1.1

7.1.4 Name Forms

The X.500 DN MAY also contain domain component attributes. Subject Alternative Names MAY also be used if marked “non-critical”.

For certificates issued to human subscribers, the subject DN SHALL either contain the value “Unaffiliated” in the last organizational unit (ou) attribute or SHALL contain the affiliated organization name in the appropriate relative distinguished name attribute, for example, organization (o), organizational unit (ou), or domain component (dc).

All name forms:

1. SHALL ensure distinguished names comply with RFC 5280;
2. SHALL ensure distinguished names are unique within a name space;
3. SHALL encode multiple dn values as separate relative distinguished names;
4. SHALL ensure GUIDs comply with RFC 4122;
5. SHALL include o=Boeing or o=<appropriate organization>;
6. SHALL include the o attribute exactly as it appears for the Issuing CA (e.g., o=Boeing);
7. SHALL include at least one attribute that uniquely identifies the subject (e.g., cn, serial number);
8. SHALL include c=<two-letter ISO 3166 country code of the Issuing CA>;
9. SHOULD refer to an entry in an authoritative directory;
10. SHOULD include ou;
11. SHOULD ensure distinguished names accurately reflect organizational structures.
12. SHOULD NOT include deprecated attributes in the distinguished name;
13. SHOULD NOT include data in the name that is already addressed by an attribute in the certificate; and
14. MAY include additional attributes as identified in RFC 5280.

For certificates issued to CAs, the Subject attribute:

15. SHALL include cn=Boeing <Service> <Env> CA <Gen #> or as otherwise approved (e.g. for Commercial Airlines).

For certificates issued to human subscribers, the Subject Alternative Name (SAN) attribute:

16. MAY only include Boeing e-mail addresses in the RFC 5322 or updates to RFC 5322 or superseding RFCs Name attribute;
17. MAY include the GUIDs associated with a card in the uniformResourceIdentifier attribute; and
18. MAY include user principal names in the otherName – PrincipalName attribute.

For certificates issued to non-human subscribers, the Subject Alternative Name (SAN) attribute:

19. MAY include host aliases, IP address, UPN, or a dNSName attribute.

7.1.5 Name Constraints

Boeing Root CAs:

1. SHALL assert name constraints for cross-certificates issued to another Bridge CA where:
   a. Critical=yes;
   b. excludedSubtrees field identifies name spaces restricted by the Boeing PKI Operational Authority; and
2. MAY assert name constraints in order to limit Issuing CAs to name spaces that are approved by the Boeing PKI Operational Authority.

7.1.6 Certificate Policy Object Identifier

Specific OIDs pertaining to Boeing PKI can be found in an applicable Certificate Profiles located on the PKI Repository.

Certificates issued under this CP:

1. SHALL assert one or more of the certificate policy OIDs contained within the Boeing Public Key Infrastructure arc managed by the Boeing IS PKI organization; and
2. SHALL ensure that CAs include all policy OIDs in the assurance levels that are lower than the highest policy OID asserted.

7.1.7 Usage of Policy Constraints Extension

Boeing Root CAs SHALL assert the *Inhibit Any Policy* constraint for cross-certificates issued to another Bridge CA where Critical=no; skipCerts=0.

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

Processing semantics for the certificate policy extension SHALL conform to X.509 certification path processing rules where critical=yes.

7.2 CRL Profile

CRL profiles:

1. SHALL comply with RFC 5280;
2. SHALL be a full and complete CRL covering all certificates signed by any and all keys associated with the CA if the CRL does not include issuingDistributionPoint; and
3. MAY issue partitioned CRLs as long as the CRLs are not indirect CRLs, are not partitioned by reason code, and the CRL DP and issuingDistributionPoint do not assert a name relativeToIssuer.

7.2.1 Version Numbers

The use of version numbers SHALL comply with the X.509 standard defined in RFC 5280.

7.2.2 CRL and CRL Entry Extensions

CRL extensions:

1. SHALL be marked critical=yes for required extensions;

2. SHALL be marked critical=no for any optional extensions; and
3. MAY be included as specified by RFC 5280.

CRL extensions for cross-certified certificates SHALL be marked *critical=yes* only if the intended relying parties have agreed to the use of the extension.

7.3 OCSP Profile

OCSP requests and responses:

1. SHALL be in accordance with RFC 6960; and
2. SHOULD issue a full and complete CRL (i.e., a CRL without issuingDistributionPoint extension) if the Entity PKI leverages the CRL to provide revocation status for its delegated OCSP services.

7.3.1 Version Numbers

The version number for responses SHALL be compliant with RFC 6960.

7.3.2 OCSP Extensions

The OCSP Extensions:

1. SHALL be compliant with RFC 6960; and
2. SHALL support the nonce extension.

8. Compliance Audit and Other Assessment

8.1 Topics Covered by Assessment

Compliance Audits:

1. SHALL evaluate practice statement assertions for conformance to the Boeing CP;
2. SHALL ensure that the procedures and controls defined in practice statements are properly implemented and enforced;
3. SHOULD follow standard auditing best practices and methodologies;
4. SHOULD consider all changes in policy, procedures, personnel, system, and/or technical aspects since a previous compliance audit;
5. SHOULD verify prior audit areas of improvement based on risk or corrective actions from the last compliance audit have been addressed; and
6. SHOULD verify previous compliance audit findings for carry-over changes and corrective actions.

Security Assessments (e.g., penetration testing, host assessments, network assessments, vulnerability assessments):

7. SHALL follow standard security assessment best practices and methodologies;
8. SHALL ensure the effectiveness of security controls; and
9. SHALL identify and apply additional security controls needed to protect against the evolving threat landscape.

8.2 Frequency or Circumstances of Assessments

Compliance Audits:

1. SHALL occur per Boeing PKI Policy Authority Chair and Boeing PKI OAA direction as stipulated in an applicable CPS; and
2. SHOULD occur when significant change (e.g., implementing a new CA, results of a security assessment recommendation) has been made to policy documentation or the operational environment.

CAs that issue medium assurance credentials have the following additional requirement:

3. SHALL occur annually for Boeing to maintain cross-certification or trust relationships.

Security Assessments:

4. SHALL occur per out-of-band Boeing company policies and procedures;
5. SHALL occur when significant change has security implications to the environment; and
6. SHALL occur when deemed warranted to verify integrity of the environment.

8.3 Identity and Qualifications of Assessor

The Compliance Auditor:

1. SHALL perform Information System Security and/or compliance audits as a primary responsibility;
2. SHALL be licensed or certified or have experience in conducting WebTrust audits for CAs, SOC2/Type II audits, or auditing Federal PKI systems; and
3. SHALL be familiar with PKI and its operations.

The Security Assessor:

4. SHALL be approved by Information Security per out-of-band Boeing company policies and procedures;
5. SHOULD perform security assessment as a primary responsibility; and
6. SHOULD be certified in the field of security assessments.

8.4 Assessor's Relationship to Assessed Entity

Compliance Audits:

1. SHALL be conducted by a Boeing PKI Policy Authority Chair/Boeing PKI OAA-approved independent third party sufficiently organizationally separated from the audited PKI to provide an unbiased, independent evaluation.

CAs that issue medium assurance credentials have the following additional compliance audit requirement:

2. SHALL undergo an audit from an external, non-Boeing third party, every third year.

Security Assessments:

3. SHALL be conducted by an approved independent third party sufficiently organizationally separated from the assessed PKI who provides an unbiased assessment.

8.5 Actions Taken as a Result of Deficiency

As a result of Compliance Audits and Security Assessments, the Compliance Auditor or Security Assessor:

1. SHALL report discrepancies and deficiencies to the Boeing PKI OAA, the Boeing PKI Policy Authority Chair and other stakeholders as needed prior to completing an audit or assessment.

The Compliance Auditor or Security Assessor, Boeing PKI OAA, Boeing PKI Policy Authority Chair and other stakeholders as needed:

2. SHALL review all reported discrepancies and deficiencies;
3. SHALL agree to discrepancies and deficiencies that require resolution;
4. SHALL develop a resolution plan;
5. SHALL communicate discrepancies, deficiencies, and final disposition to appropriate personnel or external entities;
6. SHALL resolve discrepancies and deficiencies per the resolution plan; and
7. SHALL confirm discrepancies and deficiencies are resolved.

8.6 Communication of Results

Distribution of Compliance Audits and Security Assessments results:

1. SHALL be limited to personnel with a need-to-know;
2. SHALL include the Boeing PKI Policy Authority Chair and Boeing PKI OAA;
3. SHALL include the appropriate external entities as required to maintain cross-certification or trust relationships; and
4. SHALL use appropriate controls to prevent unauthorized disclosure.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

Boeing IS PKI does not charge certificate issuance or certificate revocation fees but reserves the right to charge fees.

9.1.2 Certificate Access Fees

Boeing IS PKI does not charge certificate access fees but reserves the right to charge a fee for making a certificate available in a repository or otherwise.

9.1.3 Revocation or Status Information Access Fees

Boeing IS PKI does not charge a Revocation or Status Information Access fee but reserves the right to charge a fee for providing customized CRLs or other value-added revocation and status information services.

9.1.4 Fees for Other Services

Boeing IS PKI does not charge a fee for accessing this CP. However, any use of the CP for purposes other than viewing the document, including reproduction, redistribution, modification, or creation of derivative works, may be subject to a license agreement with the entity holding the copyright to the document.

9.1.5 Refund Policy

Not applicable.

9.2 Financial Responsibility

Acceptance of Boeing issued certificates is entirely at the discretion of the organization acting as a Relying Party. Organizations acting as relying parties SHALL determine the financial limits, if any; they wish to impose for certificates used to consummate any financial transaction. The Boeing IS PKI assumes no financial responsibility of liability for those decisions.

9.2.1 Insurance Coverage

No stipulation.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End Entities

No stipulation.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The following SHALL be kept confidential and private ("Confidential/Private Information"):

1. Certificate request records;

Commented [M(PA1]: •Consider if the below changes from other PKISaaS CP would be appropriate for this CP and then determine if we are going to need to change the BCAP CPS:

•

•In section 9.3, *Confidentiality of business information*, **MODIFY** text as follows:

~~CA information not requiring protection shall be made publicly available. Public access to organizational information shall be determined by the applicable organization.~~

9.3.1 Scope of Confidential Information

~~No stipulation.~~

Business or corporate information held by a CA or an RA which does not appear in Certificates or in public directories is considered confidential.

9.3.2Information not within the scope of Confidential Information

~~No stipulation.~~

Any information made public in a certificate is deemed not confidential. In that respect, Certificates, OCSP responses, CRLs and corporate or private information appearing in them and in public directories are not considered as private or confidential.

9.3.3Responsibility to Protect Confidential Information

~~No stipulation.~~

Each CA shall maintain the confidentiality of confidential business information that is clearly marked or labelled as confidential or by its nature should reasonably be understood to be confidential and shall treat such information with the same degree of care and security as the CA treats its own most confidential information.

Confidential business or corporate information shall not be disclosed by the CA or RA, unless required by valid law or court order.

•In section 9.4, *Privacy of personal information*, **ADD** subsections, and **MODIFY** text as follows:

~~The Boeing Company may collect, store, process and disclose personally identifiable information in accordance with The Boeing Company Personal Information Protection and Privacy Policy which designates standard methods and tools for privacy protection.~~

9.4.1Privacy Plan

The collection and storage of Personally Identifiable Information shall be limited to the minimum necessary to validate the identity of …

2. Transactional records (both full records and the audit trail of transactions);
3. Audit logs and reports;
4. Contingency planning and disaster recovery plans; and
5. Security measures (e.g., security controls, pen tests, vulnerability assessment, etc.) of the PKI.

9.3.3 Information Not within the Scope of Confidential Information

No stipulation.

9.3.2 Responsibility to Protect Confidential Information

No stipulation.

9.4 Privacy of Personal Information

The Boeing Company may collect, store, process, and disclose personally identifiable information in accordance with The Boeing Company Personal Information Protection and Privacy Policy, which designates standard methods and tools for privacy protection.

9.5 Intellectual Property Rights

The Boeing Company retains exclusive rights to any products or information developed under or pursuant to this CP.

9.6 Representations and Warranties

Representations and warranties contained in commercial agreements between Boeing and other parties may be contained in the following documents:

1. Master Services Agreement(s);
2. Memorandums of Agreement(s); or
3. Trust Agreement(s).

9.7 Disclaimers of Warranties

To the extent permitted by applicable law, Boeing disclaims all warranties with respect to certificates, including but not limited to, ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS; ANY IMPLIED WARRANTY ARISING FROM COURSE OF PERFORMANCE, COURSE OF DEALING OR USAGE OF TRADE; ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY IN TORT, WHETHER OR NOT ARISING FROM THE NEGLIGENCE OF BOEING; AND ANY OBLIGATION, LIABILITY, RIGHT, CLAIM OR REMEDY FOR LOSS OF OR DAMAGE TO ANY AIRCRAFT.

9.8 Limitations of Liability

A NON-BOEING SUBSCRIBER OR ENTITY SHALL HAVE NO CLAIM AGAINST BOEING ARISING FROM OR RELATING TO ANY CERTIFCIATE ISSUED BY A BOEING CA OR A CA’S DETERMINATION TO TERMINATE A CERTIFICATE. BOEING SHALL NOT BE LIABLE FOR ANY RELATED LOSSES, INCLUDING DIRECT OR INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, OR PUNITIVE DAMAGES.

NOTWITHSTANDING ANYTHING HEREIN TO THE CONTRARY, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL BOEING BE LIABLE FOR ANY INDIRECT DAMAGES OF ANY KIND, INCLUDING CONSEQUENTIAL, INCIDENTAL, SPECIAL, PUNITIVE, OR OTHER DAMAGES WHATSOEVER ARISING OUT OF OR RELATED TO THIS CP, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE TOTAL, AGGREGATE LIABILITY OF BOEING FOR ALL CLAIMS ARISING OUT OF OR RELATED TO ITS IMPROPER ACTIONS SHALL NOT EXCEED ONE MILLION DOLLARS ($1 MILLION USD).

9.9 Indemnities

No stipulation.

9.10 Term and Termination

9.10.1 Term of this CP

No stipulation.

9.10.2 Provisions for Termination

Termination of this CP is at the discretion of the Boeing PKI Policy Authority Board.

9.10.3 Consequences of Termination

Upon termination of this CP, PKI participants are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates.

9.11 Individual Notices and Communications with Participants

PKI participants SHALL use commercially reasonable methods to communicate with each other, considering the criticality and subject matter of the communication.

9.12 Amendments

9.12.1 Procedure for Amendment

This CP's amendment procedure:

1. SHALL require a review of this CP at least once every year;
2. SHALL ensure material amendments are submitted to the Boeing PKI OAA through the Boeing PKI Change Board;
3. SHALL ensure requested material amendments are peer reviewed and incorporated into the CP appropriately;
4. SHALL ensure material amendments are reviewed and approved by the Boeing PKI Policy Authority Board;
5. SHALL preserve the Boeing PKI OAA's right to amend the CP without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URLs, and changes to contact information;
6. SHALL preserve the Boeing PKI Policy Authority Board's (and the Boeing PKI OAA as their delegate) sole discretion to designate amendments as material or nonmaterial;
7. SHALL make notification of non-material amendments by CP publication in the PKI Repository; and
8. MAY provide to potentially affected parties (e.g., subscribers and relying parties) notice of proposed amendments, a comment period, and a mechanism by which comments are received, reviewed and if approved incorporated into this CP.

9.12.2 Circumstances under Which OIDs Must Be Changed

The Boeing PKI Policy Authority Chair or the Boeing PKI OAA:

1. SHALL determine if changes to the Boeing PKI Certificate Policy object identifiers (OIDS) are required.

If it is determined a change to a Boeing PKI OID is necessary, the Boeing PKI OAA:

2. SHALL ensure all stakeholders' representatives are informed;
3. SHALL assign a new OID;
4. SHALL ensure, if needed, policy mappings (e.g., affecting cross-certificates, retiring OIDs) are updated; and
5. SHALL ensure supporting documentation, certificate profiles (templates), and the PKI Repository are updated.

9.13 Dispute Resolution Procedures

No stipulation.

9.14 Governing Law

The enforceability, construction, interpretation, and validity of this CP for all purposes shall be governed by United States Federal law (statute, case law, or regulation), or if not applicable, by the laws of the State of Delaware, U.S.A.

9.15 Compliance with Applicable Law

This CP is subject to applicable national, state, local, and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information.

9.16 Miscellaneous Provisions

No stipulation.

9.16.1 Entire Agreement Clause

No stipulation.

9.16.2 Assignment Clause

No stipulation.

9.16.3 Severability Clause

In the event that a clause or provision of this CP is held to be unenforceable by a court of law or other tribunal having authority, the remainder of the CP shall remain valid.

9.16.4 Enforcement Clause

No stipulation.

9.16.5 Force Majeure Clause

No stipulation.

9.17 Other Provisions

No stipulation.

Appendix A: Bibliography

Some of the below references are only accessible to employees of The Boeing Company.

124-15-00000	Boeing Cryptographic Standards Document
FIPS 140-2	Security Requirements for Cryptographic Modules May 25, 2001
FIPS 186-2	Digital Signature Standard, January 27, 2000
FIPS 186-4	Digital Signature Standard (DSS), July 2013
ISO 9594-8	RECOMMENDATION ITU-T X.509
NIST Glossary	Computer Security Resource Center, Glossary
NIST SP 800-63	Digital Identity Guidelines
NIST SP 800-88	Guidelines for Media Sanitization
NIST SP 800-131A	Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths
RFC 5322	Internet Message Format (IMF)
RFC 3647	Certificate Policy and Certification Practices Framework, Chokhani and Ford, Sabett, Merrill, and Wu, November 2003
RFC 2119	Keywords Used to Indicate Requirement Importance
RFC 6960	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
RFC 4122	A Universally Unique IDentifier (UUID) URN Namespace
RFC 5280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile